APLICACIÓN DE PENTESTING A LA RED DE LA SECRETARIA DE EDUCACION DE SOGAMOSO

WILSON ESCOBAR LEMUS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SOGAMOSO
2017

APLICACIÓN DE PENTESTING A LA RED DE LA SECRETARIA DE EDUCACION DE SOGAMOSO.

WILSON ESCOBAR LEMUS
C.C. 9396906

Trabajo de grado:
Investigación aplicada para optar el título de
Especialista en Seguridad Informática.

Director de proyecto: ING. JULIO VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SOGAMOSO
2017

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

ANEXO DE TABLAS

INTRODUCCIÓN

La seguridad informática es una disciplina que permite proteger la información de una organización, proporciona herramientas que pueden ser aplicadas para evitar ser víctima de un delito informático, el objetivo de la seguridad informática es garantizar la integridad, disponibilidad y autenticidad de la información. El proyecto expuesto a continuación permite realizar un análisis de riesgos y vulnerabilidades a que está expuesta la red LAN de la Secretaria de Educación y Cultura de Sogamoso, utilizando herramientas de seguridad informática que permitan identificar los fallos y así generar los correctivos necesarios para proteger la información garantizando la seguridad de la información, tomando esto como parte de las responsabilidades de los administradores de la red y las personas encargadas de la seguridad de la información. Para comprobar la seguridad de la red se realizarán las pruebas de penetración con el programa NMAP herramienta de código abierto bajo licencia GPL para la explotación y auditoria de seguridad en redes TCP/IP, diseñada para escanear de forma rápida y eficaz. Se utilizará la interfaz gráfica multiplataforma y libre; *Zenmap* soportada oficialmente por los desarrolladores de *Nmap*, es una aplicación gráfica para manejar *Nmap* que permite escáner los puertos y obtener información al respecto.

1 TITULO

APLICACIÓN DE PENTESTING A LA RED DE LA SECRETARIA DE EDUCACION DE SOGAMOSO.

2 DEFINICION DEL PROBLEMA

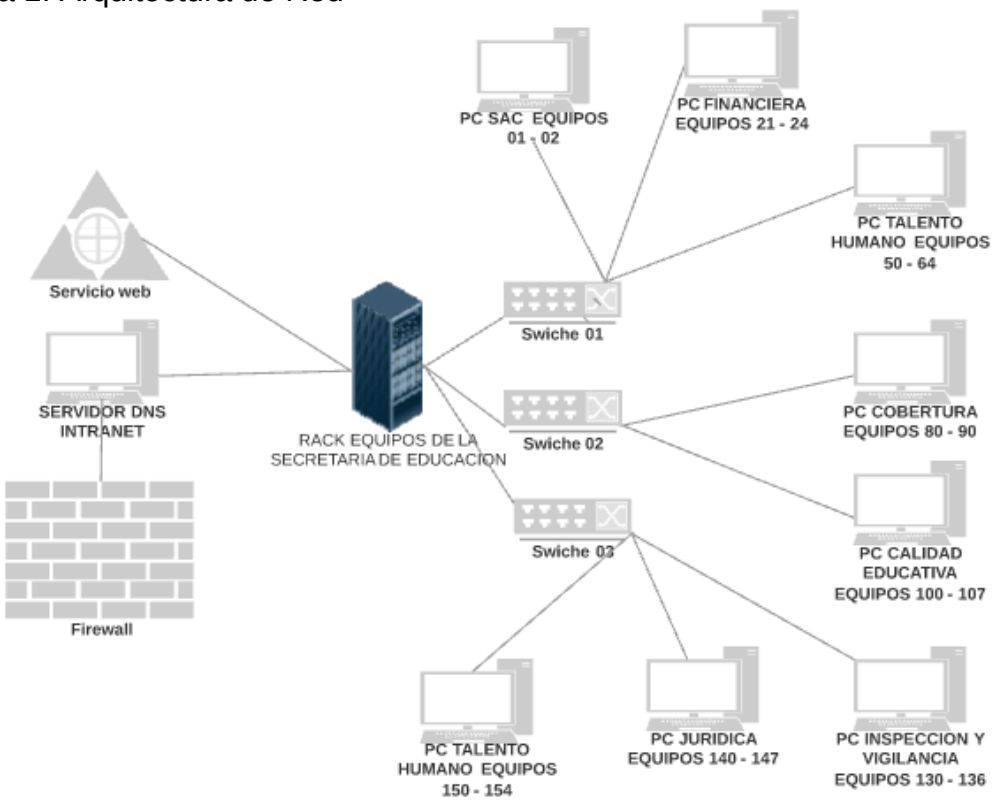
2.1 ANTECEDENTES DEL PROBLEMA

La información en aplicaciones y datos es el principal activo de cualquier organización, de manera que es de vital importancia manejar altos niveles de seguridad, integridad y confiabilidad, generalmente las redes pueden ser vulneradas por personal no autorizado o empleados de la misma organización, pueden acceder a información confidencial. La Secretaria de Educación de Sogamoso es una entidad pública, que gestiona todo lo relacionado al área de educación del municipio, como son los nombramientos de maestros, nómina, ascensos de acuerdo a sus categorías, prestaciones sociales, infraestructura educativa, calidad en la educación, talento humano, cobertura educativa, entre otros, maneja diferentes tipos de aplicativos como Soporte Lógico Humano, Sineb, Simat, Sac, Sigce, Sicied, en los cuales se genera información que debe resguardarse con seguridad, sin embargo no existe garantía en relación a los datos y aplicaciones que allí manejan, no poseen un proceso que documente la seguridad de la información.

2.2 DESCRIPCION DEL PROBLEMA

La Secretaria de Educación cuenta con una red donde interactúan aproximadamente 60 equipos en red “como se evidencia en la figura 1. Arquitectura de Red,” la cual está administrada por un servidor, se requiere un análisis para diagnosticar las vulnerabilidades presentes en dicha red como son verificar el estado de puertos y servicios presentes, sistemas operativos, presencia de cortafuegos, direcciones IP y otros elementos presentes en la red**,** se debe estimar del riesgo e impacto relacionados, identificar qué servicios se están ejecutando en un dispositivo remoto, así como la identificación de equipos activos.

Figura 1. Arquitectura de Red



Fuente del autor

2.3 FORMULACION DEL PROBLEMA

¿Qué mecanismos de protección y seguridad se pueden implementar a la red de sistemas de la Secretaria de Educación y cultura de Sogamoso?

3 JUSTIFICACIÓN

La seguridad es uno de los aspectos más importantes de cualquier organización, ya que la información que las mismas poseen, constituye el activo más importante para el desarrollo de las actividades, por lo que se deben tomar todas las medidas necesarias para resguardar esta información y no ser víctimas de intrusos o delincuentes informáticos.
En la actualidad los sistemas de información son cada vez más complejos y permanecen en constantes cambios, se debe responder a estas exigencias con gran capacidad de análisis y evaluación en especial en el área de seguridad informática, contribuyendo mediante utilización de estrategias metodológicas, que mejoren la seguridad del sistema gestionado. En este sentido hay que proteger la red de sistema contra acceso de intrusos, garantizar la confidencialidad de los datos, integridad y disponibilidad de la información.[1]

Para poder mitigar las fallas de seguridad existentes en la red de sistemas de la Secretaria de Educación es necesario realizar el proceso de *Pentesting*, con las herramientas más eficientes que se encuentren en la actualidad, para poder determinar las vulnerabilidades existentes y a la vez programar y ejecutar actividades que tienden a elevar la capacidad técnica, los conocimientos, preservación y control de la seguridad de la información.

En primer lugar se debe realizar un análisis de los riesgos y vulnerabilidades que la red LAN de la Secretaria, a través de unas herramientas que permitan identificar los fallos y así generar los correctivos necesarios para proteger la información que viaja por la red, tomando esto como parte de las responsabilidades de los administradores de la red y las personas encargadas de la seguridad de la información, escaneo para el análisis de posibles vulnerabilidades en las redes de datos, mediante mecanismos como escaneo de red, escaneo de puertos, o escaneo de aplicaciones web, encontrar puntos débiles en las bases de datos.[2]

[1]http://liacolombia.com/2011/02/%C2%BFpreparado-para-presentar-tu-proyecto-de-seguridad-informatica-ante-gerencia/.
[2] http://www.segu-info.com.ar/ataques/ataques.htm.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Establecer controles de seguridad mediante los resultados de *Pentesting* realizados a la Secretaría de Educación y Cultura de Sogamoso.

4.2 OBJETIVOS ESPECÍFICOS:

- Determinar las vulnerabilidades presentes en la red de sistemas de la secretaria de Educación y cultura por medio de un *Pentesting*

- Evaluar los resultados obtenidos en las pruebas de penetración y proponer soluciones para los riesgos encontrados.

- Detallar medidas preventivas que ayuden a mitigar fallas presentes en la red de sistemas de la Secretaria de Educación de Sogamoso.

5 MARCO DE REFERENCIA

5.1 MARCO TEORICO

Este proyecto se enfoca a establecer controles de seguridad informática mediante los resultados de *Pentesting* realizados a la Secretaría de Educación y Cultura de Sogamoso. La herramienta a utilizar es Nmap (*Network Mapper*) Mapeador de redes[3]: Es una herramienta gratuita, de código abierto bajo licencia GPL, multiplataforma, disponible para consola, y que ofrece también una interfaz gráfica para facilitar su uso. Nmap explora equipos remotos mediante secuencias de paquetes TCP/IP tanto convencionales como no convencionales, es decir, paquetes convenientemente modificados que revocarán o no una respuesta en el objetivo de la cual poder extraer información. Entre esta información se encuentra, por ejemplo: el estado de los puertos y servicios, el sistema operativo, la presencia de cortafuegos y otros elementos de red, así como del direccionamiento IP de la subred.[4]

Pruebas de Penetración.

Pruebas de Penetración de Caja Negra: Donde los *pentesters* o analistas de seguridad no tienen conocimiento del funcionamiento interno del sistema, y trabaja con la información que puede conseguir por sus propios medios, igual que lo podría hacer un delincuente informático.

Pruebas de Penetración de Caja Blanca: En este tipo de pruebas los *pentesters* o analistas de seguridad tienen total conocimiento del funcionamiento interno del sistema, y trabaja con información que puede tener acceso uno o varios empleados dentro de la organización.

Pruebas de Penetración de Caja Gris: Donde los *pentesters* o analistas de seguridad pueden tener conocimiento sobre algunos aspectos del funcionamiento del sistema y de otros no.[5]

---

[3] http://www.csirtcv.gva.es/sites/all/files/downloads/Guia_Avanzada_Nmap.pdf.

[4] https://play.google.com/books/reader?id=c8kni5g2Yv8C&printsec=frontcover&output=reader&hl=es&pg=GBS.PR5.

[5] https://www.dragonjar.org/pruebas-de-penetracion.xhtml.

Las estrategias de prueba de penetración son:

Pruebas orientadas a un objetivo***:*** Estas pruebas pueden ser desarrolladas por el personal encargado de los sistemas de la organización al igual que las pruebas de penetración.

Comprobación externa***:*** esta prueba de penetración se dirige a los servidores o equipos de la organización, son visibles externamente, incluyendo servidores de nombres de dominio (DNS), servidores de correo electrónico, servidores web o firewalls. El objetivo es averiguar si un atacante externo puede entrar y hasta dónde puede llegar una vez que ha obtenido acceso.

Pruebas a ciegas: esta prueba simula los procesos llevados a cabo por un atacante, lo cual limita la información entregada con anterioridad al personal que realiza la prueba, es conveniente dar datos básicos como el nombre de la empresa, este tipo de prueba requiere un tiempo prudente en su realización, lo cual conlleva altos valores de dinero.

Pruebas de doble ciego: Las pruebas de doble ciego toman la prueba a ciegas y la llevan un paso más allá. En este tipo de prueba de penetración, solo una o dos personas de la organización pueden ser conscientes de que se está realizando una prueba. Las pruebas de doble ciego pueden ser útiles para probar el monitoreo de seguridad y la identificación de incidentes de la organización, así como sus procedimientos de respuesta.

Técnicas de sondeo de puertos: Esta técnica es de carácter rutinario, los profesionales conocen cantidad de técnicas de sondeo y cada uno la realiza a su conveniencia de acuerdo a su criterio eligiendo la más apropiada. Dado que Nmap es libre, es una de las mejores opciones de sondeo, la única barrera que existe para ser un experto en el sondeo de puertos es el conocimiento.

Detección de sistema operativo: La herramienta Nmap es eficiente en la detección de sistemas operativos a través del protocolo TCP/IP. Nmap envía una serie de paquetes TCP al sistema remoto y analiza prácticamente todos los bits de las respuestas. Nmap compara los resultados del análisis de TCP y su orden, en el momento de encontrar coincidencias se generan los registros del sistema operativo, como la versión del ISO, el tipo de dispositivo, si es conmutador, consola de juegos etc.

La herramienta Nmap indica una URL donde puede enviar las huellas si conoce (con seguridad) el sistema operativo que utiliza el equipo si no puede acertar el sistema operativo de éste y si las condiciones son óptimas, si se encontró un puerto abierto o cerrado, con esta información se podría optimizar la herramienta.[6]

Control de tiempo y rendimiento: Este es un aspecto eficiente en Nmap donde puede escanear un sistema en una red local en décimas de segundo, puede sumarse a esto la detección de versiones que incrementan los tiempos, también puede afectar algunas configuraciones de Sistemas cortafuegos. Nmap trabaja en paralelo y tiene muchos algoritmos para acelerar estos sondeos, finalmente el usuario tiene el control del funcionamiento, con algo de experiencia un usuario de Nmap puede definir las ordenes de Nmap y así obtener información de su interés, paralelamente cumple con las limitaciones de tiempo presentes.[7]

El profesional de Sistemas tiene por objeto garantizar el tiempo de actividad, rendimiento, uso de recursos y la seguridad de los servidores que administra de forma proactiva. En las organizaciones que cuentan con diversos sistemas informáticos, se torna más compleja la administración. De esta forma, las funciones del profesional de Sistemas se dividen en roles: administrador de servidores, de bases de datos, de redes, de correo electrónico, de servidores web, de seguridad, de respaldo etc. Cada uno con sus correspondientes tareas específicas.

Los ataques en redes se ejecutan con el objetivo de encontrar vulnerabilidades en protocolos y/o servicios y ejecutar desde ahí diversas tareas que a su vez pueden resultar molestas.[8]

Al igual que pasa con los programas, un sistema poco documentado será muy complicado de mantener en el tiempo. Por ello es importante que el profesional de sistemas sea capaz de documentar correctamente las tareas que realice, con el fin de poder conocer en cualquier momento la situación de cualquier componente del sistema.

Como en el testeo este tipo de tareas requieren de la participación de un cierto número de personas, el profesional debe ser capaz de realizar pruebas para asegurarse del correcto funcionamiento del sistema en general o de algún

[6] https://nmap.org/man/es/man-os-detection.html
[7] https://es.slideshare.net/juanestebanpuertacano/pruebas-de-penetracin-nmap
[8] http://manpages.ubuntu.com/manpages/trusty/es/man1/nmap.1.html

componente del mismo. Esas pruebas deben ser exhaustivas, tratando de encontrar todos los fallos posibles.

Nmap continúa actualizándose con las últimas tecnologías para mejorar el proceso de desarrollo brindando soluciones a un gran número de profesionales, reduciendo el riesgo de troyanos, *snooping*, y continúa mejorando su velocidad en el escaneo de redes, al igual que los motores *snock* aumentan el rendimiento en el sistema Windows.

5.2 MARCO CONCEPTUAL

5.2.1 Herramientas de Nmap. Nmap cuenta con una serie de herramientas funcionales que permite el sondeo de redes.

5.2.1.1 Nmap: Herramienta. Para la explotación y auditoria de seguridad en redes TCP/IP, diseñada para escanear de forma rápida, y eficaz redes de gran tamaño. Es una herramienta gratuita, de código abierto bajo licencia GPL, multiplataforma.[9]

5.2.1.2 Nping. Generador de paquetes, analizador de respuestas y medidor de tiempos de respuesta. Permite generar paquetes de un gran rango de protocolos, permitiendo a los usuarios manipular virtualmente cualquier campo de las cabeceras de los protocolos. Además de ser usado como una simple utilidad de ping, *Nping* puede ayudar, como generador de paquetes en bruto, a tareas como pruebas de strés, envenenamiento ARP, rastreo de rutas, ataques de denegación de servicio, etcétera. [10]

5.2.1.3 Ncat. Re-implementación de la conocida herramienta *Netcat.* Es una herramienta de red que transporta paquetes entre distintas redes. Se ha diseñado para ser una herramienta robusta que pueda proveer de conectividad a otras aplicaciones y usuarios. Permite, por ejemplo, re direccionar tráfico de puertos TCP y UDP a otros destinos, ser utilizado como Proxy HTTP, incluso con autenticación, etc.

[9] https://www.dragonjar.org/como-realizar-un-pentest.xhtml.
[10] http://www.hackplayers.com/2015/11/llega-la-version-7-de-nmap.html

5.2.1.4 Ndiff. Herramienta para la comparación de diferentes análisis realizados por Nmap. A partir de los ficheros de salida de dos análisis diferentes sobre la misma red, muestra las diferencias existentes entre ellos. Es de utilidad para mostrar cambios recientes en redes con análisis periódicos.

5.2.1.5 Zenmap. Interfaz gráfica multiplataforma y libre, soportada oficialmente por los desarrolladores de NMap. Su objetivo es facilitar a los principiantes el uso de la aplicación, mientras provee funcionalidades avanzadas para usuarios más experimentados.[11]

5.2.2 Tecnologías. En general las tecnologías destinadas a la seguridad en sistemas de información son utilizadas para la protección de sistemas de información.

5.2.2.1 Escáner de Puertos. Un escáner de puertos es una herramienta de seguridad destinada Principalmente a la búsqueda de puertos abiertos en una máquina remota. Habitualmente es utilizado tanto por administradores, como ayuda en la tarea de análisis de la seguridad de sus redes, como por usuarios malintencionados, para intentar comprometer las redes y acceder a recursos y servicios no autorizados. Nmap es un ejemplo escáner de puertos avanzado.[12]

5.2.2.2 Analizador de protocolos. Un capturador de tráfico de red es una herramienta de seguridad capaz de interceptar y registrar el tráfico que pasa a través de una red de datos. Es habitual que sean utilizadas en combinación con un analizador de protocolos, capaz de decodificar y analizar si el contenido de las capturas cumple con alguna especificación o estándar particular. Las aplicaciones más comunes de estas herramientas son: análisis de problemas de red, detección de intentos de intrusión, obtención de información para realizar una intrusión, monitorización del uso de la red, extracción de estadísticas de red, depuración de aplicaciones de comunicaciones, e incluso la obtención de información sensible no protegida. *WinPcap* y *tcpdump* son ejemplos de capturadores de tráfico, mientras que *WireShark* , que utiliza las anteriores para capturar tráfico, es el analizador de protocolos más utilizado[13].

[11] https://www.kalerolinex.com/wp-content/uploads/2015/01/Guia_Avanzada_Nmap.pdf?cv=1 página 9.
[12] http://www.csirtcv.gva.es/sites/all/files/downloads/Guia_Avanzada_Nmap.pdf
[13] http://www.hackplayers.com/2015/11/llega-la-version-7-de-nmap.html

5.2.2.3 Cortafuegos. Es un sistema informático, simple o compuesto, residente en una máquina, o como elemento de interconexión de redes, que actúa de punto de conexión segura entre otros sistemas informáticos. Un cortafuego se sitúa, a modo de frontera, entre dos o más redes con la finalidad de hacer cumplir unas determinadas directivas de seguridad sobre la comunicación entre ellas, constituyéndose como el mecanismo básico para la prevención y detección de amenazas de seguridad. *Iptables* es un ejemplo de cortafuegos.

5.2.2.4 IDS/IPS. (Sistema de detección/prevención de intrusiones): Un sistema de detección de intrusiones (IDS) es una herramienta que analiza el tráfico de red y en base a unas reglas predefinidas, identifica comportamientos maliciosos e intentos de explotación no autorizada de recursos. Si además de identificar, el dispositivo tiene la capacidad de bloquear el tráfico que constituye el ataque, se trata entonces de un sistema de prevención de intrusiones (IPS). *Snort* es un ejemplo de este tipo de herramienta. Generalmente estos sistemas son independientes, pero actualmente están evolucionando e introduciéndose como parte de las propias aplicaciones a proteger, en lo que se viene a llamar cortafuegos de nivel de aplicación.

5.3 MARCO LEGAL.

"Muchos sistemas presentan vulnerabilidades de seguridad que son explotados para acceder a archivos, obtener privilegios o alterar información con diferentes fines, se debe Identificar los controles y políticas para desarrollar estrategias en una organización para la seguridad Informática y se debe reconocer las diferentes vulnerabilidades a que puede estar expuesta la Secretaria actualmente. Existen organismos en el ámbito nacional e internacional encargado de apoyar en la implementación de soluciones además de conocer la legislación nacional e internacional encargada de los aspectos éticos, informáticos y el cuidado de la información.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 Protección de la información y de los datos donde se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

A continuación se indicarán algunas conductas las cuales están tipificadas como delitos informáticos según la ley Colombiana"[14].

[14] http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

“De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

5.3.1 Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

5.3.2 Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

5.3.3 Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

5.3.4 Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales.”[15]

[15] http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

5.3.5 “Obstaculización ilegitima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes

5.3.6 Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.” [16]

“Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala por quien tuviere un vínculo contractual con el poseedor de la información”. Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal. Por su parte, el capítulo segundo establece:

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.
La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí

[16] http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_1273_DE_2009.pdf

señalada se incrementará en la mitad. Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos o telemáticos. Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea.

En este sentido y desde un punto de vista empresarial, la nueva ley pone de presente la necesidad para los empleadores de crear mecanismos idóneos para la protección de uno de sus activos más valiosos como lo es la información.

Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información.

Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo o los trabajos desde la residencia de los trabajadores los cuales exigen un nivel más alto de supervisión al manejo de la información.
Así mismo, resulta conveniente dictar charlas y seminarios al interior de las organizaciones con el fin de que los trabajadores sean conscientes del nuevo rol que les corresponde en el nuevo mundo de la informática.

Lo anterior, teniendo en cuenta los perjuicios patrimoniales a los que se pueden enfrentar los empleadores debido al uso inadecuado de la información por parte de sus trabajadores y demás contratistas.

Pero más allá de ese importante factor, con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.”[17].

5.4 MARCO ESTADO ACTUAL DE LA EMPRESA.

[17] http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

La Secretaria de Educación de Sogamoso es una entidad pública que Gestiona todo lo relacionado al área de educación del municipio, como son los nombramientos de maestros, nómina, ascensos de acuerdo a sus categorías, prestaciones sociales, infraestructura educativa, calidad en la educación, talento humano, cobertura educativa. Su función principal es administrar y garantizar el Derecho al servicio público educativo en sus diferentes modalidades y niveles, enmarcado dentro de las políticas de equidad, cobertura, calidad y eficiencia, caracterizando las principales necesidades de la comunidad educativa para articularlas con los planes, programas y proyectos educativos con el propósito de lograr una gestión de calidad en la educación de la ciudad de Sogamoso. Entre sus principales objetivos esta laborar, promover y ejecutar el Plan de Desarrollo Educativo del Municipio, sobre la base del acuerdo, el consenso la participación de toda la comunidad educativa, el cual debe considerar como objetivo, mejorar la cobertura, la calidad, la modernización de la educación, diagnosticar, dirigir, controlar y evaluar la prestación del servicio público educativo de competencia municipal, ofrecido tanto por las instituciones estatales como los de carácter privado y solidario, enmarcándolos en las políticas trazadas por el Ministerio de Educación.[18]

La secretaria de Educación está estructurada por dependencias como Inspección y vigilancia que se encarga de realizar las actividades de apoyo, desarrollo, análisis y verificación, relacionadas con la ejecución de los procesos de auditoría de matrícula e inspección y vigilancia, Calidad educativa, apoya administrativamente y complementar el desarrollo de las actividades asociadas con la gestión de la calidad educativa. Sac - servicio de atención al ciudadano ejecuta los procesos administrativos de la dependencia, entre otros.

5.5 MARCO TECNOLÓGICO

La Secretaria de Educación y Cultura de Sogamoso maneja diferentes tipos de aplicativos como Soporte Lógico Humano, Sineb, Simat, Sac, Sigce, Sicied, entre otros de los cuales se genera información de vital importancia para la Secretaria, además cuenta con una serie de equipos de cómputo y servidores, a los cuales se desconoce si se realiza sus respectivos mantenimientos, no se evidencia un sistema de protección y Seguridad Informática, que garantice la seguridad en el manejo de la información. La Secretaria de Educación y Cultura cuenta con una red LAN, está compuesta por cableado y canaleta que cumplen las normas técnicas, 60 computadores todos en red, 8 impresoras de las cuales 4 están en red, 2 escáner y sistema operativo Windows 7.

[18] http://sem-sogamoso-boyaca.gov.co

6 DISEÑO METODOLOGICO

6.1 TIPO DE INVESTIGACION

El siguiente proyecto está orientado a brindar protección contra las contingencias y riesgos relacionados con la seguridad de la información en la red de sistemas de la secretaria de Educación y cultura, para lo cual se va a realizar una investigación aplicada, cuyo objetivo es determinar el problema a través de la práctica a través de la observación y la experimentación de la aplicación de los test de penetración a la red y técnicas de análisis de los contenidos.

6.2 INSTRUMENTOS

Este proyecto se vale de los siguientes recursos

6.2.1 Investigación por encuesta. Práctica a través de la observación y la experimentación de la aplicación de los test de penetración a la red y técnicas de análisis de los contenidos a través de entrevistas con los funcionarios de la Secretaria de Educación y Cultura.

6.2.2 Técnicas de análisis de datos Se elaboró una encuesta de tipo dicotómicas es decir con respuestas sí o no, la cual fue aplicada a los funcionarios de la Secretaria de Educación y Cultura de Sogamoso.

6.2.3 Población y muestra. Para el caso de investigación de la Secretaria de Educación y Cultura de Sogamoso, la muestra debe ser representativa en donde se determina la población que tiene acceso a los sistemas de información que se tendrá en cuenta para el estudio de la seguridad en la red.

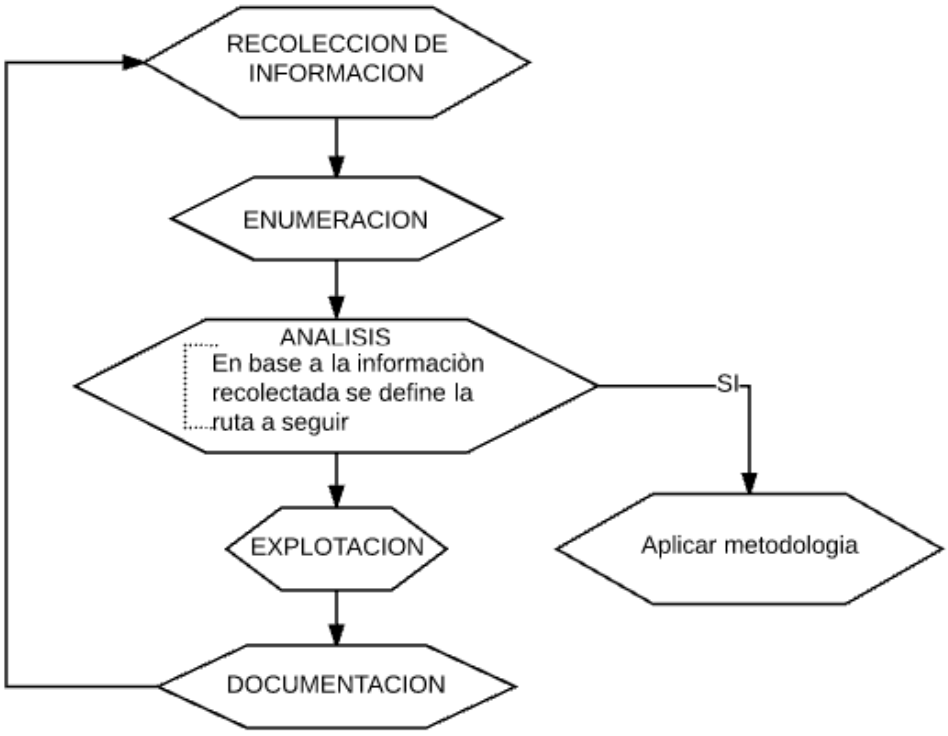
6.2.3.1 Población. Funcionarios de la Secretaria de Educación y Cultura de Sogamoso

6.2.3.2 Muestra. Representantes de área de la Secretaría.

6.3 METODOLOGIA DE DESARROLLO.

Para la aplicación del *Pentesting* o *Test* de Penetración, se desarrolló un procedimiento metodológico y sistemático “como se evidencia en la Figura 2. Diagrama Metodológico”, donde se simula un ataque real a la red de la Secretaria de Educación y Cultura de Sogamoso, con el fin de determinar el nivel de seguridad informática de tal forma que se pueda adoptar mecanismos de protección y formular recomendaciones o estrategias orientadas a su seguridad. Para la metodología utilizada en este *pentesting* se tomaron aspectos relevantes de OSSTMM *(Open Source Security Testing Methodology Manual*) del instituto para la seguridad y las metodologías abiertas ISECOM, la Guía de pruebas OWASP, ISSAF (*Information Systems Security Assassment Framework*) y *Penetration Testing Framework de Vulnerability Assessment* las cuales se integran para para realizar cada una de las etapas del *Pentesting*.[19]

Figura 2. Diagrama Metodológico



Fuente del autor

[19] http://www.dragonjar.education/curso/como-se-realiza-un-pentest/

6.3.1 Recolección de información. Las siguientes son las técnicas de recolección de información que se tomaron en consideración durante la ejecución del proyecto:

6.3.1.1 Información de la empresa. La Secretaria de Educación de Sogamoso es una entidad pública que Gestiona todo lo relacionado al área de educación del municipio, como son los nombramientos de maestros, nómina, ascensos de acuerdo a sus categorías, prestaciones sociales, infraestructura educativa, calidad en la educación, talento humano, cobertura educativa.

- Misión. Administrar y garantizar el Derecho al servicio público educativo en sus diferentes modalidades y niveles, enmarcado dentro de las políticas de equidad, cobertura, calidad y eficiencia, caracterizando las principales necesidades de la comunidad educativa para articularlas con los planes, programas y proyectos educativos con el propósito de lograr una gestión de calidad en la educación de la ciudad de Sogamoso.:[20]

- Visión. En el año 2017, la Secretaría de Educación del Municipio de Sogamoso será una Entidad destacada en los primeros lugares a nivel nacional por contar con procesos pedagógicos, administrativos y tecnológicos modernos y certificados, a través de los cuales se garantice la calidad y la pertinencia del servicio educativo, en armonía con el proceso de globalización.[21]

- Políticas: Con el ánimo de asegurarse de medir y controlar el SGC frente al servicio que se presta se han definido los siguientes Políticas de acuerdo con las funciones y niveles pertinentes de operación:

- Establecer programas de educación para adultos, a través de convenios con los establecimientos educativos públicos y privados para beneficiar a 700 personas anualmente.

- Suscribir convenios interinstitucionales para desarrollar 4 programas educativos que promuevan la mentalidad empresarial en el municipio.

[20] http://sem-sogamoso-boyaca.gov.co

- Garantizar en un 80% la adopción y ejecución de los planes de mejoramiento aprobados para cada institución educativa oficial y privada.

- Implementar en el 100% de las instituciones públicas y privadas el proceso pedagógico de la cátedra Suamox.

- Legalizar y controlar el cumplimiento de los programas en cuanto a duración, calidad y tipo de certificación que expidan la totalidad de las instituciones de educación no formal.

- Establecer un programa anual de capacitaciones para directivos, docentes y personal administrativo, con un 100% de asistencia de las instituciones educativas oficiales.

- Mejorar anualmente los promedios en las pruebas del ICFES y ubicarnos dentro de los mejores 10 municipios certificados del país.

- Implementar el bibliobanco en cada una de las 16 instituciones, para garantizar la formación de los jóvenes.

- Conformar la red de bibliotecas públicas municipales.

- Mejorar el 30% de la infraestructura educativa del sector oficial del municipio.

- Desarrollar un sistema de comunicación virtual que contribuya al desarrollo de la región.

- El 60% de los estudiantes comprenderá la importancia de las normas, de las leyes y del estado para el fortalecimiento de las competencias ciudadanas.

- Atender el 100% de las oportunidades de mejora y problemas detectados dentro de la gestión de mejora continua.

- Objetivos de la secretaria de educación de Sogamoso.

- “Elaborar, promover y ejecutar el Plan de Desarrollo Educativo del Municipio, sobre la base del acuerdo, el consenso la participación de toda la comunidad educativa, el cual debe considerar como objetivo, mejorar la cobertura, la calidad, la modernización de la educación

- Diagnosticar, dirigir, controlar y evaluar la prestación del servicio público educativo de competencia municipal, ofrecido tanto por las instituciones estatales como los de carácter privado y solidario, enmarcándolos en las políticas trazadas por el Ministerio de Educación.

- Identificar y priorizar las necesidades de infraestructura y dotación educativa en coordinación con la Secretaría de Infraestructura y Valorización.

- Elaborar técnicamente los proyectos educativos e inscribirlos en el Banco de Proyectos Municipal, Departamental, Nacional.

- Promover la elaboración de estudios e investigaciones en el contexto local y regional de la problemática educativa para proponer políticas, programas, proyectos y estrategias en los aspectos estructurales y organizacionales.

- Dirigir y coordinar la aplicación de políticas para la administración del personal del sector educativo.

- Dependencias. La Secretaria de Educación está estructurada por dependencias “como se evidencia en la Figura 4. Estructura organizacional de la Secretaria de Educación y Cultura de Sogamoso “las cuales esta orientadas por unos objetivos específicos en pro de una Calidad Educativa basada en la Excelencia

- Inspección – vigilancia. Realizar las actividades de apoyo, desarrollo, análisis y verificación, relacionadas con la ejecución de los procesos de auditoría de matrícula e inspección y vigilancia, tanto en los Establecimientos Educativos como

en la SEC; lo anterior, cumpliendo con los parámetros de calidad establecidos en el plan operativo anual de inspección y vigilancia."[22]
Aplicar los conocimientos propios de su formación profesional para la ejecución de actividades misionales de control en el área de inspección y vigilancia.
Cargo**:** Director de Núcleo/ líder inspección y vigilancia.

- Calidad educativa. Apoyar administrativamente y complementar el desarrollo de las actividades asociadas con la gestión de la calidad educativa. Apoyar la promoción de los resultados de las evaluaciones como insumos para el perfeccionamiento de los planes de mejoramiento con actividades administrativas y operativas de manejo de documentos, seguimiento a los planes de asistencia técnica pedagógica.
Cargo: Profesional de Calidad

- SAC - Servicio de Atención al Ciudadano. Ejecutar los procesos administrativos de la dependencia, indispensables para el desarrollo de la gestión, administrando un sistema de información física y magnética que sirva de soporte documental, teniendo en cuenta las políticas de la Entidad.
Cargo Profesional del Área.

- Cobertura educativa. Apoyar administrativamente y complementar el desarrollo de las actividades asociadas con la gestión de cobertura del servicio educativo y el análisis de la información relacionada con acceso y permanencia.
Cargo Profesional del Área

- Planeación. Apoyar operativamente la recopilación de información y las actividades relacionadas con la ejecución de los procesos asociados a la Gestión Estratégica de la Secretaría de Educación, la Gestión de Programas, Proyectos y la Administración del Sistema de Gestión de Calidad.
Cargo Profesional del Área

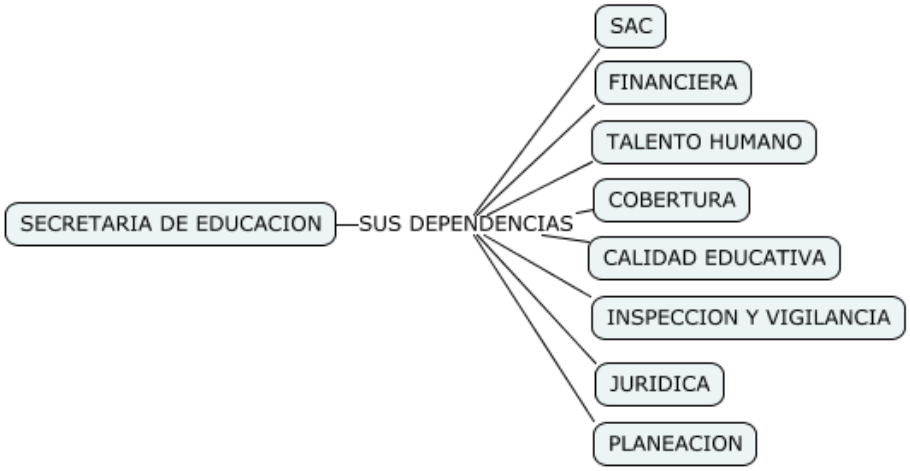
- Talento humano. Radicar, verificar, clasificar y registrar o dar trámite a las novedades que impactan la inscripción, actualización y ascenso en el escalafón docente y en la carrera administrativa, a los trámites del fondo de prestaciones sociales y custodiar y mantener el archivo de hojas de vida del personal docente, directivo docente y administrativo de acuerdo a las normas y procedimientos vigentes.

[22]http://sem-sogamoso-boyaca.gov.co

Cargo: Líder del área

6.3.1.2 Estructura organizacional de la secretaria de educación y cultura de Sogamoso.

Figura 3. Estructura organizacional de la Secretaria de Educación y Cultura de Sogamoso



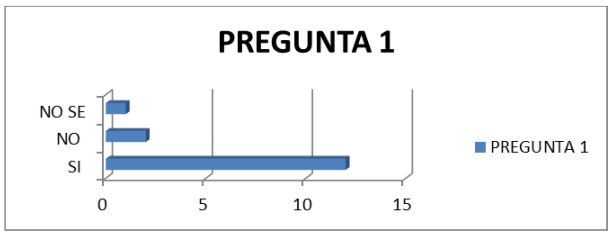
Fuente del autor.

6.3.1.3 Resultados y análisis de la aplicación de la encuesta.

1. Usted tiene conocimiento acerca de que es la seguridad Informática?
   Si 12 No 2 No sé 1

SI: 80%
NO 13%
NO SE 7%

Figura 4. Pregunta 1



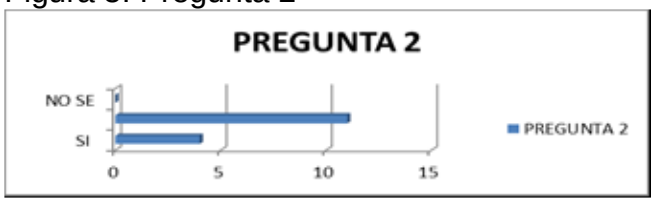
Fuente del autor.

Se evidencia en la Figura 5. Pregunta 1 que la mayoría de los funcionarios tienen el conocimiento al respecto de la seguridad informática.

2. Conoce algún plan de seguridad informática implementado en la secretaria de Educación y cultura de Sogamoso.
   Si 4 No 11 No Sé 0

SI: 27%
NO 73%
NO SE 0%

Figura 5. Pregunta 2



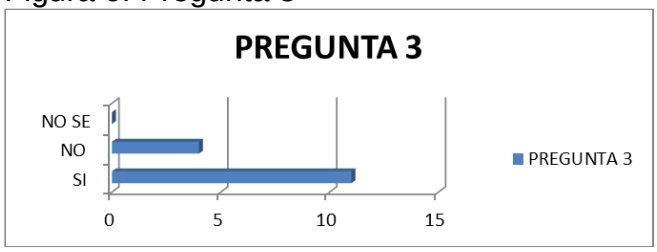
Fuente del autor.

Se evidencia en la Figura 6. Pregunta 2, que se desconoce si esta implementado un plan de Seguridad informática.

3. Usted ha permitido el acceso a la información que maneja sólo a personas debidamente autorizadas?
   Si 11 No 4 No sé 0

SI: 73%
NO 27%
NO SE 0%

Figura 6. Pregunta 3



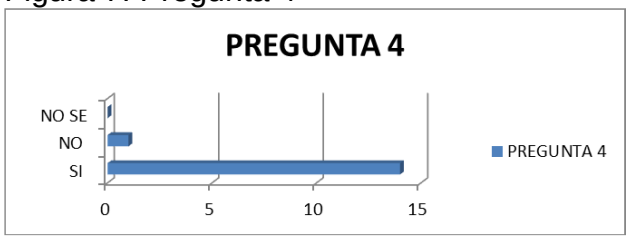
Fuente del autor.

Se evidencia en la Figura 7. Pregunta 3, que la información la maneja solo las personas autorizadas

4. ¿la información que usted maneja tiene los privilegios de confidencialidad, integridad y disponibilidad?
   Si 14 No 1 No sé 0

SI: 93%
NO 7%
NO SE 0%

Figura 7. Pregunta 4



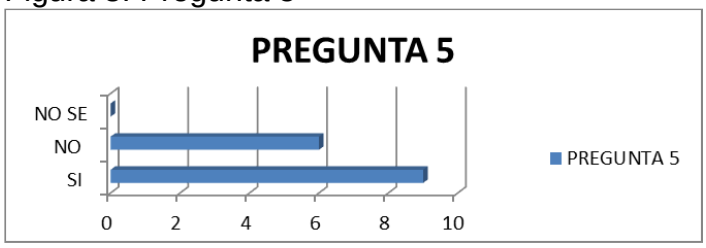
Fuente del autor.

Se evidencia en la Figura 8. Pregunta 4, que Reconocen que la información tiene los privilegios de confidencialidad, integridad y disponibilidad

5. Usted como usuario ha accedido a todos los datos permitidos?
   Sí 9 No 6 No sé 0

SI: 60%
NO 40%
NO SE 0%

Figura 8. Pregunta 5



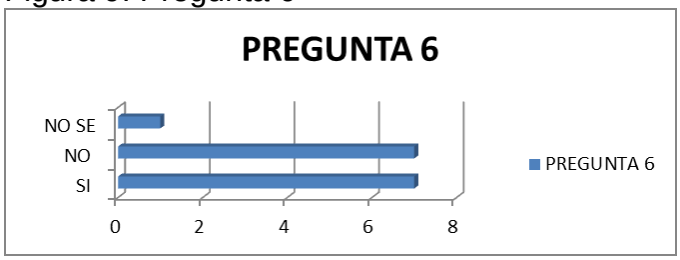
Fuente del autor.

Se evidencia en la Figura 9. Pregunta 5 que la mayoría ha accedido a los datos permitidos.

6. Se tiene definida una política para las copias de seguridad de la información?
   Si 7 No 7 No sé 0

SI: 47%
NO 47%
NO SE 7%

Figura 9. Pregunta 6



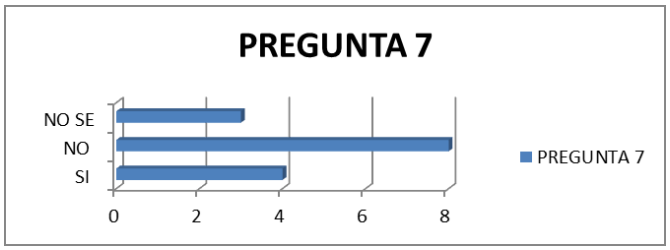
Fuente del autor.

Se evidencia en la Figura 10. Pregunta 6 que la muestra está dividida en el conocimiento de las políticas de copias de seguridad.

7. Se tiene definida una política de restauración de los sistemas en caso de ataques informáticos?
   Sí 4 No 8 No sé 3

SI: 27%
NO 53%
NO SE 20%

Figura 10. Pregunta 7



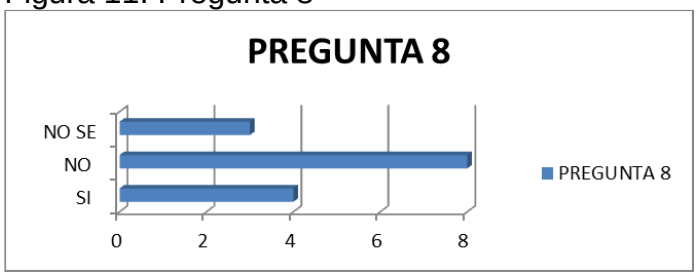
Fuente del autor.

Se evidencia en la Figura 11. Pregunta 7 que la mayoría desconoce una política de restauración de copias de seguridad.

8. Tiene conocimiento acerca de algún tipo de seguridad en la red?
   Sí 4 No 8 No sé 3

SI: 27%
NO 53%
NO SE 20%

Figura 11. Pregunta 8



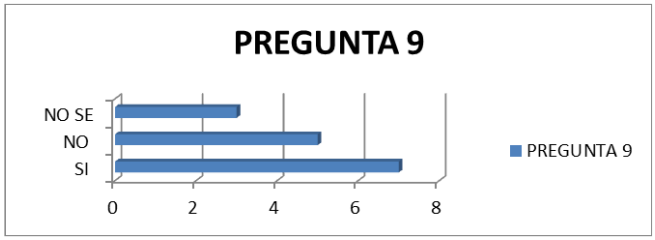
Fuente del autor.

Se evidencia en la Figura 12. Pregunta 8 que no tiene conocimiento de seguridad en red.

9. La Secretaría cuenta con antivirus actualizado?
   Sí 7 No 5 No sé 3

SI: 47%
NO 33%
NO SE 20%

Figura 12. Pregunta 9



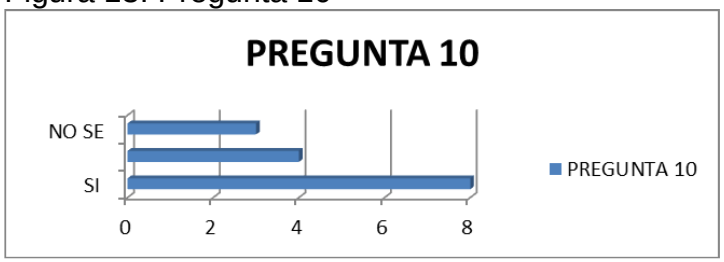
Fuente del autor.

Se evidencia en la Figura 13. Pregunta 9 que la mayoría tiene conocimiento de antivirus actualizado.

10. La secretaria cuenta un control de las claves de los computadores?
Sí 8 No 4 No sé 3

SI: 53%
NO 27%
NO SE 20%.

Figura 13. Pregunta 10



Fuente del autor.

Se evidencia en la Figura 14. Pregunta 10 que la mayoría tiene conocimiento de control de claves de los computadores.

6.3.2 Enumeración. La herramienta utilizada para la prueba de penetración es Nmap que es una herramienta para la explotación y auditoria de seguridad en redes TCP/IP, diseñada para escanear de forma rápida, y eficaz redes de gran tamaño. Es una herramienta gratuita, de código abierto bajo licencia GPL, multiplataforma.

Al realizar unas pruebas con Nmap se `puede obtener información como la medición de tiempo de actividad, donde se utiliza la marca de tiempo TCP (RFC 1323) que indica cuando fue reiniciado un equipo, esta prueba solo aplica para los sistemas que ofrecen esta información. Otros aspectos o pruebas que se pueden obtener es la clasificación de predicción de número de secuencia TCP. Esta prueba mide de forma aproximada cuánto de difícil es crear una conexión TCP falsa contra el sistema remoto.

Los ataques en redes se ejecutan con el objetivo de encontrar vulnerabilidades en protocolos y/o servicios y ejecutar desde ahí diversas tareas que a su vez pueden resultar molestas.

Al igual que pasa con los programas, un sistema poco documentado será muy complicado de mantener en el tiempo. Por ello es importante que el profesional de sistemas sea capaz de documentar correctamente las tareas que realice, con el fin de poder conocer en cualquier momento la situación de cualquier componente del sistema. Nmap continúa actualizándose con las últimas tecnologías para mejorar el proceso de desarrollo brindando soluciones a un gran número de profesionales, reduciendo los riesgos de troyanos y continúa mejorando su velocidad en el escaneo de redes[23].

6.3.2.1 Inventario de activos

Tabla 1. Inventario de activos

INVENTARIO DE ACTIVOS							
NOMBRE DE EQUIPO	DEPARTAMENTO	CARGO	DIRECCION IP	SERIAL DE CONTROL	TIPO	MARCA	SISTEMA OPERATIVO
SAC 01	SAC	PROFESIONAL DEL AREA	192.168.0.1	FJGCP-4DFJD-GJY49-VJBQ7-HYRR2	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 7 PROFESIONAL
SAC 02	SAC	TECNICO PROFESIONAL	192.168.0.2	|VQ3PY-VRX6D-CBG4J-8C6R2-TCVBD	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 7 ULTIMATE
FINANCIERA 01	FINANCIERA	PROFESIONAL DEL AREA	192.168.0.21	|2Y4WT-DHTBF-Q6MMK-KYK6X-VKM6G	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 10 PROFESIONAL
FINANCIERA 02	FINANCIERA	PROFESIONAL DEL AREA	192.168.0.22	|342DG-6YJR8-X92GV-V7DCV-P4K27	COMPUTADOR DE ESCRITORIO	ACER	WINDOWS 7 PROFESIONAL

[23] https://www.dragonjar.org/como-realizar-un-pentest.xhtml.

Tabla 1. (Continuación)

INVENTARIO DE ACTIVOS

NOMBRE DE EQUIPO	DEPARTAMENTO	CARGO	DIRECCION IP	SERIAL DE CONTROL	TIPO	MARCA	SISTEMA OPERATIVO
FINANCIERA 03	FINANCIERA	PROFESIONAL DEL AREA	192.168.0.23	|MHFPT-8C8M2-V9488-FGM44-2C9T3	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 PROFESIONAL
FINANCIERA 04	FINANCIERA	TECNICO PROFESIONAL	192.168.0.24	2|22TKD-F8XX6-YG69F-9M66D-PMJBM	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 PROFESIONAL
TALENTO HUMANO 01	TALENTO HUMANO	LIDER DEL AREA	192.168.0.50	|6K2KY-BFH24-PJW6W-9GK29-TMPWP	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 PROFESIONAL
TALENTO HUMANO 02	TALENTO HUMANO	PROFESIONAL DEL AREA	192.168.0.51	|49PB6-6BJ6Y-KHGCQ-7DDY6-TF7CD	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 7 PROFESIONAL
TALENTO HUMANO 03	TALENTO HUMANO	PROFESIONAL DEL AREA	192.168.0.52	|YJJYR-666KV-8T4YH-KM9TB-4PY2W	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 10 PROFESIONAL
TALENTO HUMANO 04	TALENTO HUMANO	PROFESIONAL DEL AREA	192.168.0.53	|YKHFT-KW986-GK4PY-FDWYH-7TP9F	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 7 PROFESIONAL
TALENTO HUMANO 05	TALENTO HUMANO	PROFESIONAL DEL AREA	192.168.0.54	7||4CFBX-7HQ6R-3JYWF-72GXP-4MV6W	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 PROFESIONAL
TALENTO HUMANO 06	TALENTO HUMANO	PROFESIONAL DEL AREA	192.168.0.55	|2WCJK-R8B4Y-CWRF2-TRJKB-PV9HW	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 PROFESIONAL
TALENTO HUMANO 07	TALENTO HUMANO	PROFESIONAL DEL AREA	192.168.0.56	32KD2-K9CTF-M3DJT-4J3WC-733WD	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 PROFESIONAL
TALENTO HUMANO 08	TALENTO HUMANO	PROFESIONAL DEL AREA	192.168.0.57	|PT9YK-BC2J9-WWYF9-R9DCR-QB9CK	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 PROFESIONAL
TALENTO HUMANO 09	TALENTO HUMANO	PROFESIONAL DEL AREA	192.168.0.58	|HCL|2QTV2-3CMPP-FQBYK-GRD62-D7XMW	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
TALENTO HUMANO 10	TALENTO HUMANO	PROFESIONAL DEL AREA	192.168.0.59	|74T2M-DKDBC-788W3-H689G-6P6GT	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 PROFESIONAL
TALENTO HUMANO 11	TALENTO HUMANO	PROFESIONAL DEL AREA	192.168.0.60	|237XB-GDJ7B-MV8MH-98QJM-24367	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 PROFESIONAL
TALENTO HUMANO 12	TALENTO HUMANO	TECNICO PROFESIONAL	192.168.0.61	|GMJQF-JC7VC-76HMH-M4RKY-V4HX6	COMPUTADOR DE ESCRITORIO	ACER	WINDOWS 7 ULTIMATE

Tabla 1. (Continuación)

INVENTARIO DE ACTIVOS

NOMBRE DE EQUIPO	DEPARTAMENTO	CARGO	DIRECCION IP	SERIAL DE CONTROL	TIPO	MARCA	SISTEMA OPERATIVO
TALENTO HUMANO 13	TALENTO HUMANO	TECNICO PROFESIONAL	192.168.0.62	|H9M26-6BXJP-XXFCY-7BR4V-24X8J	COMPUTADOR DE ESCRITORIO	GENERICO	WINDOWS 98
TALENTO HUMANO 14	TALENTO HUMANO	TECNICO PROFESIONAL	192.168.0.63	|2V8P2-QKJWM-4THM3-74PDB-4P2KH	COMPUTADOR DE ESCRITORIO	GENERICO	WINDOWS 98
TALENTO HUMANO 15	TALENTO HUMANO	TECNICO PROFESIONAL	192.168.0.64	|6JKVQ-WJTWW-JVPRB-77TGD-2DV7M	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
COBERTURA 01	COBERTURA	PROFESIONAL DEL AREA	192.168.0.80	862R9-99CD6-DD6WM-GHDG2-Y8M37	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 98
COBERTURA 02	COBERTURA	PROFESIONAL DEL AREA	192.168.0.81	2|7JQWQ-K6KWQ-BJD6C-K3YVH-DVQJG	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 98
COBERTURA 04	COBERTURA	PROFESIONAL DEL AREA	192.168.0.83	7|38JTJ-VBPFW-XFQDR-PJ794-8447M	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
COBERTURA 05	COBERTURA	TECNICO PROFESIONAL	192.168.0.84	|V3Y2W-CMF9W-PGT9C-777KD-32W74	COMPUTADOR DE ESCRITORIO	GENERICO	WINDOWS 98
COBERTURA 06	COBERTURA	TECNICO PROFESIONAL	192.168.0.85	|2QDBX-9T8HR-2QWT6-HCQXJ-9YQTR	COMPUTADOR DE ESCRITORIO	ACER	WINDOWS 7 ULTIMATE
COBERTURA 07	COBERTURA	TECNICO PROFESIONAL	192.168.0.86	6RBBT-F8VPQ-QCPVQ-KHRB8-RMV82	COMPUTADOR DE ESCRITORIO	ACER	WINDOWS 7 ULTIMATE
COBERTURA 08	COBERTURA	TECNICO PROFESIONAL	192.168.0.87	FJGCP-4DFJD-GJY49-VJBQ7-HYRR2	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
COBERTURA 09	COBERTURA	TECNICO PROFESIONAL	192.168.0.88	|VQ3PY-VRX6D-CBG4J-8C6R2-TCVBD	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
COBERTURA 10	COBERTURA	TECNICO PROFESIONAL	192.168.0.89	|2Y4WT-DHTBF-Q6MMK-KYK6X-VKM6G	COMPUTADOR DE ESCRITORIO	GENERICO	WINDOWS 98
COBERTURA 11	COBERTURA	TECNICO PROFESIONAL	192.168.0.90	|342DG-6YJR8-X92GV-V7DCV-P4K27	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 7 ULTIMATE

Tabla 1. (Continuación)

INVENTARIO DE ACTIVOS

NOMBRE DE EQUIPO	DEPARTAMENTO	CARGO	DIRECCION IP	SERIAL DE CONTROL	TIPO	MARCA	SISTEMA OPERATIVO
CALIDAD EDUCATIVA 01	CALIDAD EDUCATIVA	PROFESIONAL DE CALIDAD	192.168.0.100	|MHFPT-8C8M2-V9488-FGM44-2C9T3	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
CALIDAD EDUCATIVA 02	CALIDAD EDUCATIVA	PROFESIONAL DE CALIDAD	192.168.0.101	2|22TKD-F8XX6-YG69F-9M66D-PMJBM	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
CALIDAD EDUCATIVA 03	CALIDAD EDUCATIVA	PROFESIONAL DE CALIDAD	192.168.0.102	|6K2KY-BFH24-PJW6W-9GK29-TMPWP	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
CALIDAD EDUCATIVA 04	CALIDAD EDUCATIVA	PROFESIONAL DE CALIDAD	192.168.0.103	|49PB6-6BJ6Y-KHGCQ-7DDY6-TF7CD	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
CALIDAD EDUCATIVA 05	CALIDAD EDUCATIVA	TECNICO PROFESIONAL	192.168.0.104	|YJJYR-666KV-8T4YH-KM9TB-4PY2W	COMPUTADOR DE ESCRITORIO	GENERICO	WINDOWS 98
CALIDAD EDUCATIVA 06	CALIDAD EDUCATIVA	TECNICO PROFESIONAL	192.168.0.105	|YKHFT-KW986-GK4PY-FDWYH-7TP9F	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
CALIDAD EDUCATIVA 07	CALIDAD EDUCATIVA	TECNICO PROFESIONAL	192.168.0.106	7||4CFBX-7HQ6R-3JYWF-	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
CALIDAD EDUCATIVA 08	CALIDAD EDUCATIVA	TECNICO PROFESIONAL	192.168.0.107	|2WCJK-R8B4Y-CWRF2-TRJKB-PV9HW	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
INSPECCIÓN Y VIGILANCIA 01	INSPECCIÓN Y VIGILANCIA	DIRECTOR DE NUCLEO	192.168.0.130	32KD2-K9CTF-M3DJT-4J3WC-733WD	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
INSPECCIÓN Y VIGILANCIA 02	INSPECCIÓN Y VIGILANCIA	PROFESIONAL DEL AREA	192.168.0.131	|PT9YK-BC2J9-WWYF9-R9DCR-QB9CK	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
INSPECCIÓN Y VIGILANCIA 03	INSPECCIÓN Y VIGILANCIA	PROFESIONAL DEL AREA	192.168.0.132	|HCL|2QTV2-3CMPP-FQBYK-GRD62-D7XMW	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
INSPECCIÓN Y VIGILANCIA 04	INSPECCIÓN Y VIGILANCIA	PROFESIONAL DEL AREA	192.168.0.133	|74T2M-DKDBC-788W3-H689G-6P6GT	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
INSPECCIÓN Y VIGILANCIA 05	INSPECCIÓN Y VIGILANCIA	TECNICO PROFESIONAL	192.168.0.134	|237XB-GDJ7B-MV8MH-98QJM-24367	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
INSPECCIÓN Y VIGILANCIA 06	INSPECCIÓN Y VIGILANCIA	TECNICO PROFESIONAL	192.168.0.135	|GMJQF-JC7VC-76HMH-M4RKY-V4HX6	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL

Tabla 1. (Continuación)

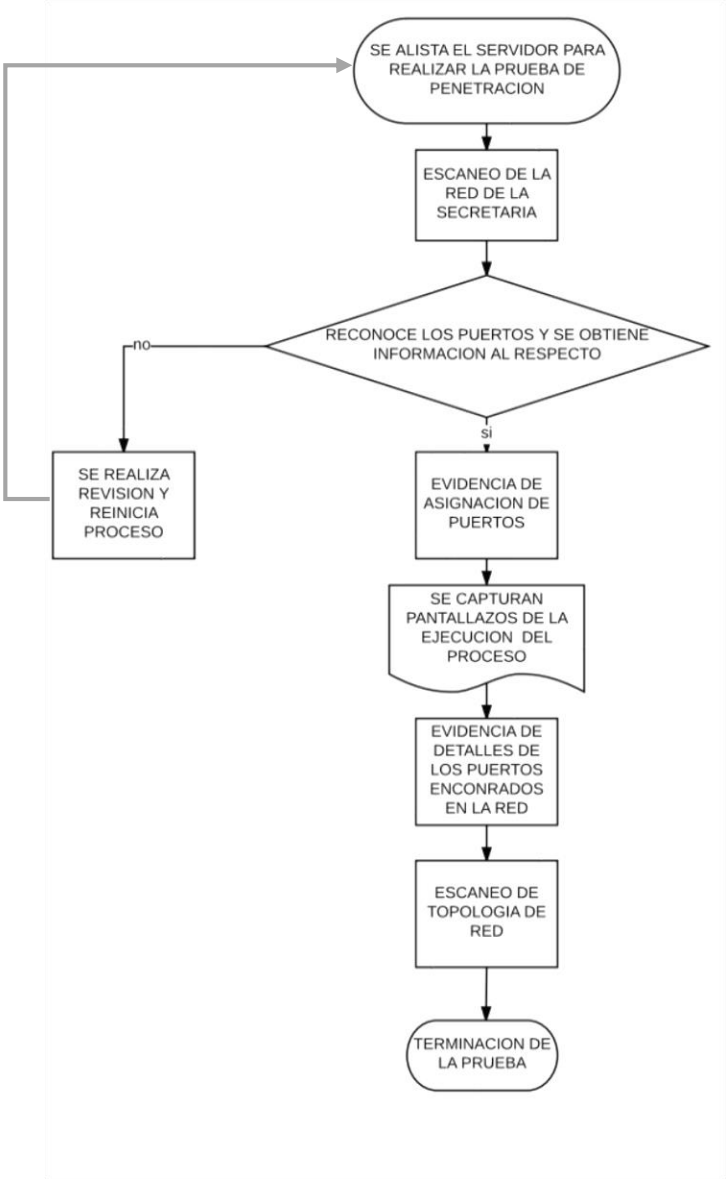
INVENTARIO DE ACTIVOS							
NOMBRE DE EQUIPO	DEPARTAMENTO	CARGO	DIRECCION IP	SERIAL DE CONTROL	TIPO	MARCA	SISTEMA OPERATIVO
INSPECCIÓN Y VIGILANCIA 07	INSPECCIÓN Y VIGILANCIA	TECNICO PROFESIONAL	192.168.0.136	|H9M26-6BXJP-XXFCY-7BR4V-24X8J	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
JURIDICA 01	JURIDICA	SECRETARIO DE EDUCACION	192.168.0.140	|2V8P2-QKJWM-4THM3-74PDB-4P2KH	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
JURIDICA 02	JURIDICA	PROFESIONAL DEL AREA	192.168.0.141	|6JKVQ-WJTWW-JVPRB-77TGD-2DV7M	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
JURIDICA 03	JURIDICA	PROFESIONAL DEL AREA	192.168.0.142	862R9-99CD6-DD6WM-GHDG2-Y8M37	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
JURIDICA 04	JURIDICA	PROFESIONAL DEL AREA	192.168.0.143	2|7JQWQ-K6KWQ-BJD6C-K3YVH-DVQJG	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
JURIDICA 05	JURIDICA	PROFESIONAL DEL AREA	192.168.0.144	VQB3X-Q3KP8-WJ2H8-R6B6D-7QJB7	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
JURIDICA 06	JURIDICA	PROFESIONAL DEL AREA	192.168.0.145	7|38JTJ-VBPFW-XFQDR-PJ794-8447M	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
COBERTURA 03	COBERTURA	PROFESIONAL DEL AREA	192.168.0.82	VQB3X-Q3KP8-WJ2H8-R6B6D-7QJB7	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
JURIDICA 07	JURIDICA	TECNICO PROFESIONAL	192.168.0.146	|V3Y2W-CMF9W-PGT9C-777KD-32W74	COMPUTADOR DE ESCRITORIO	LENOVO	WINDOWS 7 ULTIMATE
JURIDICA 08	JURIDICA	TECNICO PROFESIONAL	192.168.0.147	FJGCP-4DFJD-GJY49-VJBQ7-HYRR2	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
PLANEACIÓN 01	PLANEACIÓN	PROFESIONAL DEL AREA	192.168.0.150	|VQ3PY-VRX6D-CBG4J-8C6R2-TCVBD	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
PLANEACIÓN 02	PLANEACIÓN	PROFESIONAL DEL AREA	192.168.0.151	|2Y4WT-DHTBF-Q6MMK-KYK6X-VKM6G	COMPUTADOR DE ESCRITORIO	HP	WINDOWS 10 PROFESIONAL
PLANEACIÓN 03	PLANEACIÓN	PROFESIONAL DEL AREA	192.168.0.152	|342DG-6YJR8-X92GV-V7DCV-P4K27	COMPUTADOR DE ESCRITORIO	GENERICO	WINDOWS 98
PLANEACIÓN 04	PLANEACIÓN	TECNICO PROFESIONAL	192.168.0.153	|MHFPT-8C8M2-V9488-FGM44-2C9T3	COMPUTADOR DE ESCRITORIO	GENERICO	WINDOWS 7 ULTIMATE
PLANEACIÓN 05	PLANEACIÓN	TECNICO PROFESIONAL	192.168.0.154	2|22TKD-F8XX6-YG69F-9M66D-PMJBM	COMPUTADOR DE ESCRITORIO	GENERICO	WINDOWS 7 ULTIMATE

Fuente del autor.

6.3.3 Análisis. Ya obteniendo la información en la etapa enumeración, se toman decisiones para llegar al objetivo.

6.3.3.1 Diagrama de flujo enfocados al uso

Figura 14. Diagrama de flujo enfocados al uso



Fuente del autor.

6.3.3.2 Análisis y evaluación de seguridad acerca de las vulnerabilidades presentes en la red de sistemas de la secretaria de educación y cultura.

Por lo general los ataques informáticos se generan a causa de malas configuraciones por parte del usuario en equipos y sistemas operativos, estos pueden ser solucionados a corto plazo, Se debe estar actualizado acerca de los tipos de ataques que se estén presentando en la actualidad. Una forma de evitar estos ataques y cubrir las vulnerabilidades es implementar un sistema de seguridad informático en la Secretaria de Educación y cultura de Sogamoso, sistema que a futuro puede evitar cualquier tipo de ataque o daño, que pongan en peligro la integridad de la información.

Muchos sistemas están expuestos a cualquier vulnerabilidad de seguridad, que son explotados para acceder a archivos y obtener privilegios. Los usuarios no poseen contraseñas fuertes según las encuestas realizadas. Muchas puertas traseras son descubiertas en sistemas operativos, aplicaciones de software, protocolos de red, *browsers* de Internet, correo electrónico y toda clase de servicios informáticos disponibles, debilidad en contraseñas las cuales se evidenciaron en las encuestas realizadas.

Se detectaron vulnerabilidades de la red como: evidencia de los nombres de los equipos, el sistema operativo que se está usando y los puertos de los equipos, al aplicar algunos *scrips* se podría a acceder a información de los equipos como contraseñas, los cuales no pudieron ser ejecutados. Evidentemente los sistemas de información, están expuestos a un número elevado de amenazas, que aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de ataque, también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente. Incluyendo desastres que pueden ser naturales o accidentales.
Estas son algunas de las vulnerabilidades encontradas:

Ausencia de Contraseñas o de fácil detección; Los nombres de usuarios generalmente son fáciles de identificar, es importante que las contraseñas sean difíciles de descifrar.

Falta de Registros de eventos: Es importante tener actualizado un registro del sistema, debe ser respaldado y archivado, Mientras se navega en internet se está expuesto a que cualquier atacante que puede penetrar y pueda causar el daño, o altere la información.

Se encontraron puertos abiertos o sin control: Los ataques generalmente los realizan a través de los puertos, toman un puerto que este abierto donde pueden entrar y atacar, es importante establecer controles, tener abierto solo los puertos que son necesarios, los demás tenerlos cerrados.

Copias de Respaldo o Backups: Deben realizarse de forma periódica dependiendo la organización, debe existir una política de respaldo y restauración, revisarse por lo menos una vez al mes si se está realizando el respectivo respaldo a prueba de fallos.

Códigos maliciosos: como troyanos, virus informáticos, gusanos, spyware, etc.

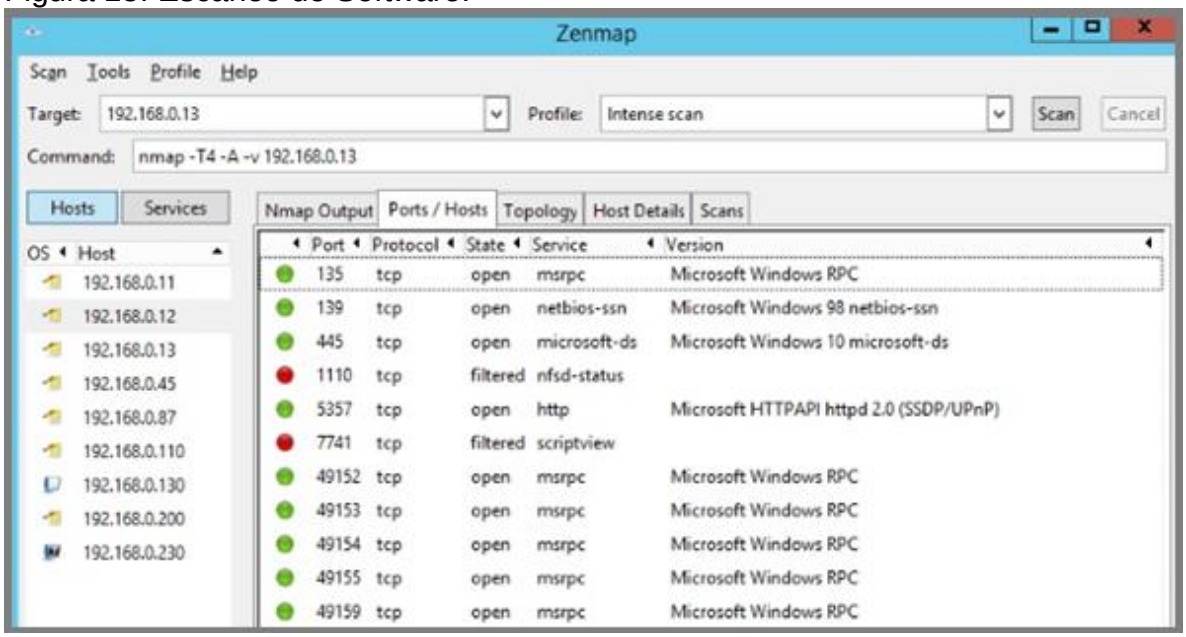
Una vez realizada la Encuesta aplicada a los funcionarios de la SECRETARIA DE EDUCACIÓN Y CULTURA DE SOGAMOSO, y luego de realizar la respectiva tabulación y obtener resultados los cuales demostró que se encuentran grandes falencias relacionadas con la seguridad de la información , seguridad en los sistemas operativos y en las redes, que se pueden evidenciar en los resultados de la encuesta, se procedió como primera instancia a programar y realizar una Socialización o Asesoría relacionada a la Seguridad Informática resaltando la importancia de la implementación de Un plan de Gobierno de las tecnologías de Información, resaltando las vulnerabilidades a las que están expuestos, los diferentes riesgos potenciales y la importancia de estos procesos para la Secretaria.[24]

6.3.4 Explotación. Esta etapa determina los fallos de seguridad encontrados y evidencias para la realización del informe.

Se presentara los resultados obtenidos en el desarrollo del proyecto y resultados de la aplicación del pentesting aplicado a la red de la secretaria de Educación de Sogamoso para determinar el nivel de seguridad informática y a su vez se destacarán los diferentes hallazgos relacionados con dicho proyecto proponiendo establecer controles de seguridad para mitigar los posibles riesgos a la cual puede estar expuesta la red de la secretaria.[25]

[24] http://revista.seguridad.unam.mx/numero-18/pruebas-de-penetraci%C3%B3n-para-principiantes-5-herramientas-para-empezar
[25] https://www.dragonjar.org/como-realizar-un-pentest.xhtml

Figura 15. Escaneo de Software.

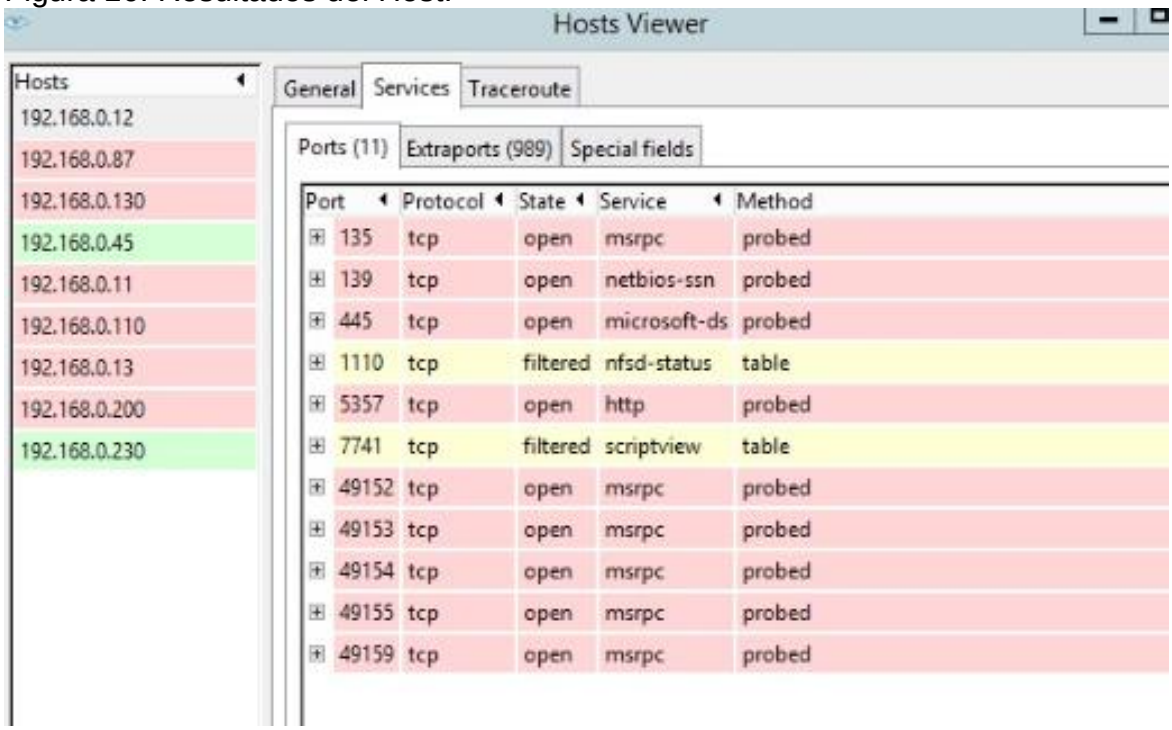


Fuente del autor.

Se evidencia en la Figura 17. Escaneo de Software que los puertos abiertos están señalados de color verde, lo cual genera gran vulnerabilidad para los equipos ya que están expuestos a un sinnúmero de amenazas para el sistema. El puerto 135 lo comparten DCOM, programador de tareas y MSDTC, al parecer se tiene alguno de estos servicios el puerto permanece abierto y aceptando conexiones entrantes. Los puertos 139 y 445, los equipos tienen *NetBios* habilitado, si *NetBios* está deshabilitado, sólo se escuchará mediante el puerto 445.

Algunas de las vulnerabilidades encontradas son ausencia de Contraseñas o de fácil detección, falta de Registros de eventos, puertos abiertos o sin control.

Figura 16. Resultados del Host.



Fuente del autor.

Copias de Respaldo o *Backups*: Deben realizarse de forma periódica dependiendo la organización, debe existir una política de respaldo y restauración, revisarse por lo menos una vez al mes si se está realizando el respectivo respaldo a prueba de fallos.

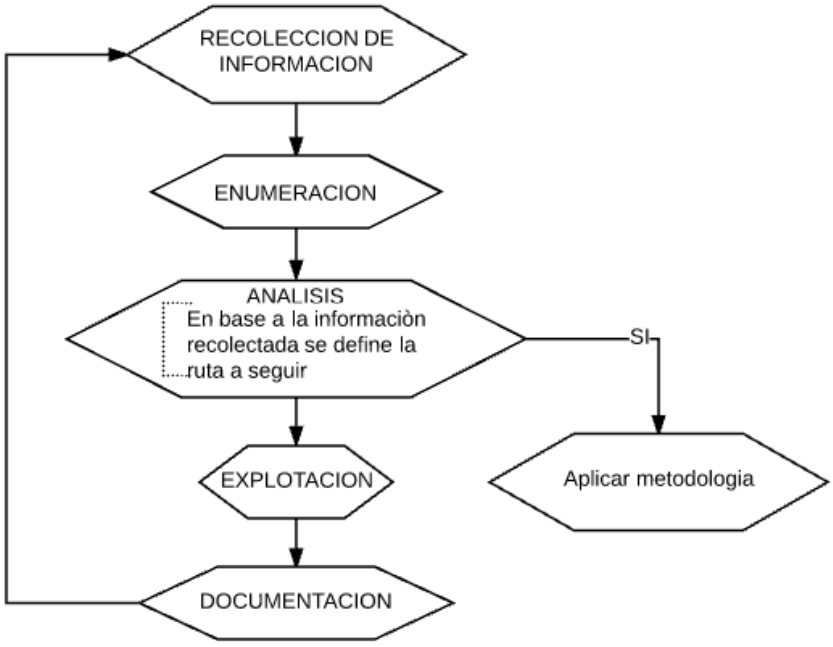
6.3.5 Documentación. Se da inicio a realizar la documentación para presentar la propuesta de la auditoria de seguridad informática aplicada a la red de la Secretaria de Educación de Sogamoso. Se debe demostrar las diversas vulnerabilidades que posea la red a ser analizada, realizando pruebas de penetración en un entorno controlado que permita señalar efectivamente las deficiencias de seguridad para poder analizarlas.[26]

[26] https://www.dragonjar.education/leccion/introduccion-al-pentesting-documentacion/

6.3.5.1 Resumen ejecutivo. El presente documento define los resultados obtenidos de la aplicación de un Pentesting a la red LAN de la Secretaria de Educación y Cultura de Sogamoso, el cual permite realizar un análisis de riesgos y vulnerabilidades a que está expuesta la red, utilizando herramientas de seguridad informática que permitan identificar los fallos y así generar los correctivos necesarios para proteger la información garantizando la seguridad de la información. Para comprobar la seguridad de la red se realizaran las pruebas de penetración con el programa NMAP herramienta de código abierto bajo licencia GPL para la explotación y auditoria de seguridad en redes TCP/IP, diseñada para escanear de forma rápida y eficaz.

- Metodología. Para la aplicación del Pentesting o Test de Penetración, se desarrolló un procedimiento metodológico y sistemático como se evidencia en la figura 17. Diagrama Metodológico, donde se simula un ataque real a la red de la Secretaria de Educación y Cultura de Sogamoso, con el fin de determinar el nivel de seguridad informática de tal forma que podamos adoptar mecanismos de protección y formular recomendaciones o estrategias orientadas a su seguridad las cuales se integran para realizar cada una de las etapas del Pentesting.[27]

Figura 17. Diagrama Metodológico



Fuente del autor

[27] https://www.dragonjar.org/como-realizar-un-pentest.xhtml

- Resultados de la prueba

Se detectaron vulnerabilidades de la red como: evidencia de los nombres de los equipos, el sistema operativo que se está usando y los puertos de los equipos, al aplicar algunos scrips se podría a acceder a información de los equipos como contraseñas, los cuales no pudieron ser ejecutados por la restricción del administrador del sistema.

Estas son algunas de las vulnerabilidades encontradas:

- Ausencia de Contraseñas o de fácil detección; Los nombres de usuarios generalmente son fáciles de identificar, es importante que las contraseñas sean difíciles de descifrar.

- Falta de Registros de eventos: Es importante tener actualizado un registro del sistema, debe ser respaldado y archivado, Mientras se navega en internet se está expuesto a que cualquier atacante que puede penetrar y pueda causar el daño, o altere la información.

- Se encontraron puertos abiertos o sin control: Los ataques generalmente los realizan a través de los puertos, toman un puerto que este abierto donde pueden entrar y atacar, es importante establecer controles, tener abierto solo los puertos que son necesarios, los demás tenerlos cerrados.

- Copias de Respaldo o Backups: Deben realizarse de forma periódica dependiendo la organización, debe existir una política de respaldo y restauración, revisarse por lo menos una vez al mes si se está realizando el respectivo respaldo a prueba de fallos.

- Códigos maliciosos: son códigos generados para crear vulnerabilidades en sistemas, los cuales crean puertas traseras y pueden generar grandes daños e inconvenientes en una organización,

En General se encuentran grandes falencias relacionadas con la seguridad de la información, seguridad en los sistemas operativos y en las redes, que se pueden evidenciar en los resultados de la encuesta[28]

- Recomendaciones y controles de seguridad acerca de las vulnerabilidades presentes en la red de sistemas de la secretaria de educación y cultura.

La Secretaria de Educación y Cultura debe programar y ejecutar actividades que tiendan a elevar la capacidad técnica, los conocimientos y preservación control que los riesgos de la seguridad de la información, así como de los sistemas involucrados en el proceso de la organización.

La Secretaria de Educación y Cultura debe contar con un Sistema de Gestión de la Seguridad de la Información SGSI que garantice un control que los riesgos de la seguridad de la información los cuales deben ser reconocidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, y eficiente. Esto se puede asociar según la norma ISO 27001, dice que dicha seguridad, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas involucrados en el proceso de la organización.

La Secretaria de Educación y Cultura debe implementar un sistema de Riesgo para garantizar la seguridad de la información y se gestione correctamente y mantenga los niveles de competitividad, rentabilidad e imagen de la Secretaria de Educación y Cultura y así lograr los objetivos.

Los profesionales de la Secretaria de Educación y cultura, deben contar con certificaciones como la del estándar COBIT (*Control Objectives for Information and related Technology*), que ofrece un conjunto de mejores prácticas para la gestión de sistemas de información garantizando la confidencialidad, integridad y disponibilidad de la información.

- Resultado de capacitaciones de mejora al personal de la Secretaria de Educación y Cultura de Sogamoso

[28] https://www.dragonjar.org/como-realizar-un-pentest.xhtml

Se realizó una capacitación al personal de la Secretaria de Educación y Cultura de Sogamoso en aras de adoptar y mantener un proceso adecuado en el manejo y mantenimiento de seguridad informática, con el fin de identificar, mitigar y prevenir fallas o perdida de información en cada una de las áreas, la cual se solicitó fuera extensiva a todo el personal de la secretaria.

La capacitación, se realizó haciendo énfasis, en el cuidado de la información de los equipos como claves y estar presto a las diferentes técnicas de ataques informáticos y diferentes vulnerabilidades que puedan presentarse,

Etapas de un ataque informático;

- Reconocimiento: Permite al atacante analizar y recolectar toda la información a través Ingeniería social, es decir accesar a información como teléfonos, correos, contraseñas, de tal forma que pueda crear una estrategia para su ataque.

- Exploración: Con la información de reconocimiento ya identificadas las vulnerabilidades determinar por donde atacar.

Obtener Acceso: Esta es la etapa de penetración al sistema informático ya explora las vulnerabilidades encontradas.

- Mantener Acceso: una vez obtenido el acceso, la idea es mantenerlo, utiliza el sistema informático para enviar nuevos ataques, hace uso de *sniffers* para capturar el tráfico de la red, *roodkit* que son herramientas que ocultan procesos, sesiones y conexiones.

- Borrar huellas: Destruye la evidencia de los rastreos, para continuar sus actividades y así no ser descubierto.

Tipos de ataques informáticos: Existen diferentes tipos de ataques informáticos, los cuales son realizados por *Hackers*. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc. Los ataques pueden utilizar sus permisos para alterar archivos o registros, ingresar a la red simplemente validando un *password*.

- Ataque de ingeniería Social: Esta forma de ataque es una de las más comunes que se presentan, ocurre cuando se aprovechan de los funcionarios a través de algún tipo de engaño, utilizan varias técnicas como es rastrear la información, exploración y enumeración, de esta forma obtienen información valiosa para el atacante como son números de documentos, , nombres de usuarios, claves, contraseñas, de esta forma pueden acceder a información con fines delictivos. Estos tipos de ataques se pueden generar a través de correos electrónicos con los cuales solicitan información como claves de acceso, la persona que envía este correo falsifican su posición de funcionario (como auditor, o técnico en mantenimiento del área, etc.), de tal forma que pueden engañar fácilmente su objetivo.

- Códigos maliciosos: Son amenaza para cualquier organización, estos son programas que pueden causar daño en los sistemas informáticos pueden ser; troyanos, virus informáticos, gusanos, *spyware, keyloggers* y muchos más, se expanden a través de USB, por correos electrónicos o mensajería, redes, vienen camuflados en diferentes aplicaciones como juegos en flash, protectores de pantalla, diferentes tipos de archivos.

- Suplantación Web: se produce cuando un atacante genera o crea otro sitio web similar al que visita la víctima, y atreves de esta ubica enlaces donde la victima entra creyendo que está haciendo uso de su página original, aquí el atacante se aprovecha de las vulnerabilidades del navegador, acostumbran también utilizar un nombre de dominio similar al de la página que están replicando.

- Ataques de fuerza bruta: trata de usar un gran número de combinaciones de letras y números o caracteres para detectar una contraseña, existen en internet muchísimas herramientas que facilitan este proceso.

- Ataques de denegación de servicios: Este tipo de ataque utilizan la tecnología como medio para engañar a la víctima, supuestamente la victima piensa que está entrando a un recurso de internet, pero realmente está entrando al del atacante y allí obtienen información o los datos de la víctima.

Cómo defenderse de estos Ataques.

Por lo general los ataques informáticos se generan a causa fallas en la seguridad de los diferentes equipos informáticos especialmente en protocolos y sistemas operativos, es conveniente estar actualizados de los tipos de ataques que se estén

presentando en la actualidad. Aunque la mejor forma de contrarrestar estos ataques y cubrir las vulnerabilidades de es contar con un óptimo sistema de seguridad informático, el cual se podrá implementar a la secretaria con un bajo costo que a futuro puede representar grandes ventajas en relación a cualquier tipo de que pongan en peligro la información.

El personal comprendió la importancia del cuidado de la información de la secretaria, que se requiere de la elaboración sistemática de actividades que tienden a elevar la capacidad técnica, los conocimientos y las destrezas del personal para ocupar posiciones de responsabilidad, se entendió que en la actualidad los sistemas de información son cada vez más complejos y permanecen en constantes cambios y se debe responder a estas exigencias con gran capacidad de análisis, contribuyendo mediante utilización de estrategias metodológicas y dinámicas a la generación de habilidades técnicas, y humanas.

La Secretaria debe tener presente que lo más importante para ella es la información la cual puede verse vulnerable debido a varias situaciones como; incendios, fallas de disco, virus, robos u otros. Esta información se debe proteger a través de copias de seguridad o también llamados Backups.

Finalmente, Se sugirió implementar un Sistema de gestión de seguridad de la información.

7 RESULTADOS Y DISCUSION

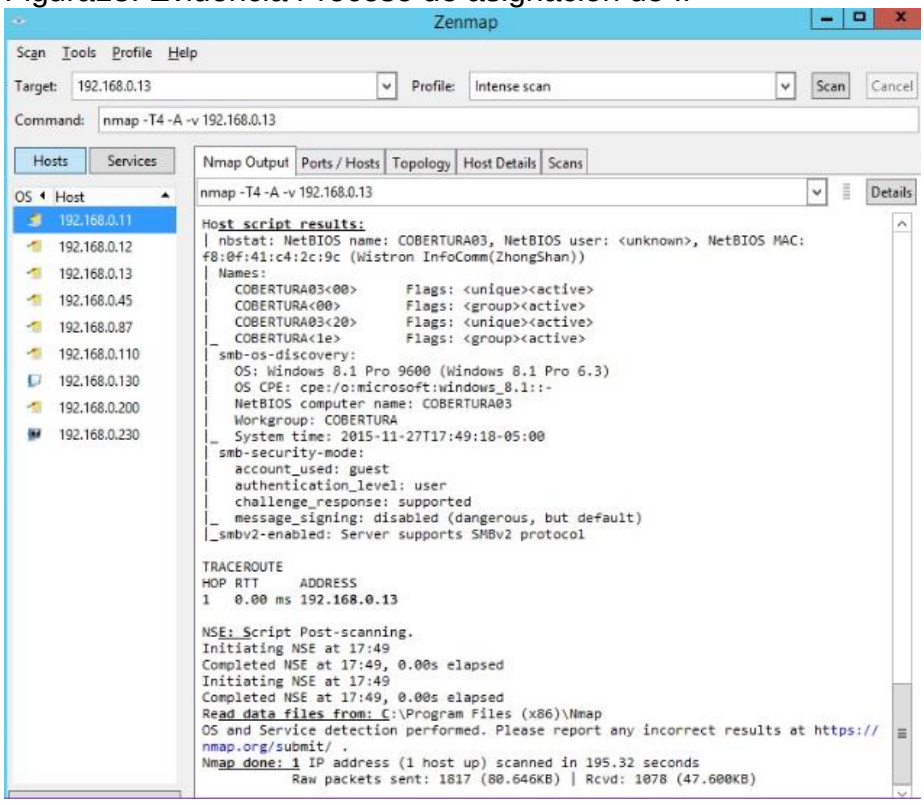
Es función del administrador de los sistemas, resguardar la información de la empresa, mantener la seguridad de la plataforma y hacerla lo menos vulnerable posible se debe tener constancia en revisión y mantenimiento en la red de los equipos de cómputo y sistemas de información.

Se descargó Nmap de la página oficial, se instala la versión 7.0.0

Zenmap: Interfaz gráfica multiplataforma y libre, soportada oficialmente por los desarrolladores de NMap. Es una aplicación gráfica para manejar Nmap que permite escáner los puertos y obtener información al respecto.

Se asigna la dirección IP de la maquina desde donde se realiza el escaneo, y se encuentran las IP de estos equipos, los demás por la hora están apagados.

Figura18. Evidencia Proceso de asignación de IP



Fuente del autor.

Se evidencia el escaneo de Nmap:

Starting Nmap 7.00 (https://nmap.org) at 2015-11-26 18:10 Hora est. Pacífico, Sudamérica
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:46
Completed NSE at 17:46, 0.00s elapsed
Initiating NSE at 17:46
Completed NSE at 17:46, 0.00s elapsed
Initiating ARP Ping Scan at 17:46
Scanning 192.168.0.13 [1 port]
Completed ARP Ping Scan at 17:46, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:46
Completed Parallel DNS resolution of 1 host. at 17:46, 0.06s elapsed
Initiating SYN Stealth Scan at 17:46
Scanning 192.168.0.13 [1000 ports]
Discovered open port 445/tcp on 192.168.0.13
Discovered open port 135/tcp on 192.168.0.13
Discovered open port 139/tcp on 192.168.0.13
Discovered open port 80/tcp on 192.168.0.13
Discovered open port 443/tcp on 192.168.0.13
Increasing send delay for 192.168.0.13 from 0 to 5 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.0.13 from 5 to 10 due to max_successful_tryno increase to 6
Warning: 192.168.0.13 giving up on port because retransmission cap hit (6).
Discovered open port 49156/tcp on 192.168.0.13
Discovered open port 49152/tcp on 192.168.0.13
Discovered open port 49158/tcp on 192.168.0.13
Discovered open port 5357/tcp on 192.168.0.13
Discovered open port 49153/tcp on 192.168.0.13
Discovered open port 49157/tcp on 192.168.0.13
Discovered open port 49155/tcp on 192.168.0.13
Discovered open port 49154/tcp on 192.168.0.13
Completed SYN Stealth Scan at 17:47, 46.10s elapsed (1000 total ports)
Initiating Service scan at 17:47
Scanning 13 services on 192.168.0.13
Service scan Timing: About 38.46% done; ETC: 17:49 (0:01:26 remaining)
Completed Service scan at 17:49, 108.64s elapsed (13 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.13
NSE: Script scanning 192.168.0.13.
Initiating NSE at 17:49
Completed NSE at 17:49, 35.46s elapsed

Initiating NSE at 17:49
Completed NSE at 17:49, 0.00s elapsed
Nmap scan report for 192.168.0.13
Host is up (0.00s latency).
Not shown: 981 closed ports
PORT STATE SERVICE VERSION
80/tcp open http
| http-methods:
|_ Supported Methods: GET
|_http-title: Site doesn't have a title.
|_xmlrpc-methods: ERROR: Script execution failed (use -d to debug)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows 98 netbios-ssn
443/tcp open https
| http-methods:
|_ Supported Methods: GET
|_http-title: Site doesn't have a title.
|_xmlrpc-methods: ERROR: Script execution failed (use -d to debug)
445/tcp open microsoft-ds Microsoft Windows 10 microsoft-ds
636/tcp filtered ldapssl
873/tcp filtered rsync
1110/tcp filtered nfsd-status
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
7741/tcp filtered scriptview
16993/tcp filtered amt-soap-https
20005/tcp filtered btx
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
49157/tcp open msrpc Microsoft Windows RPC
49158/tcp open msrpc Microsoft Windows RPC
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
MAC Address: F8:0F:41:C4:2C:9C (Wistron InfoComm(ZhongShan))
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows

8, or Windows 8.1 Update 1
Uptime guess: 1.004 days (since Thu Nov 26 17:44:42 2015)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows 98, Windows 10; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_10

Host script results:
| nbstat: NetBIOS name: COBERTURA03, NetBIOS user: <unknown>, NetBIOS MAC: f8:0f:41:c4:2c:9c (Wistron InfoComm(ZhongShan))
| Names:
| COBERTURA03<00> Flags: <unique><active>
| COBERTURA<00> Flags: <group><active>
| COBERTURA03<20> Flags: <unique><active>
|_ COBERTURA<1e> Flags: <group><active>
| smb-os-discovery:
| OS: Windows 8.1 Pro 9600 (Windows 8.1 Pro 6.3)
| OS CPE: cpe:/o:microsoft:windows_8.1::-
| NetBIOS computer name: COBERTURA03
| Workgroup: COBERTURA
|_ System time: 2015-11-27T17:49:18-05:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT ADDRESS
1 0.00 ms 192.168.0.13
NSE: Script Post-scanning.
Initiating NSE at 17:49
Completed NSE at 17:49, 0.00s elapsed
Initiating NSE at 17:49
Completed NSE at 17:49, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 195.32 seconds

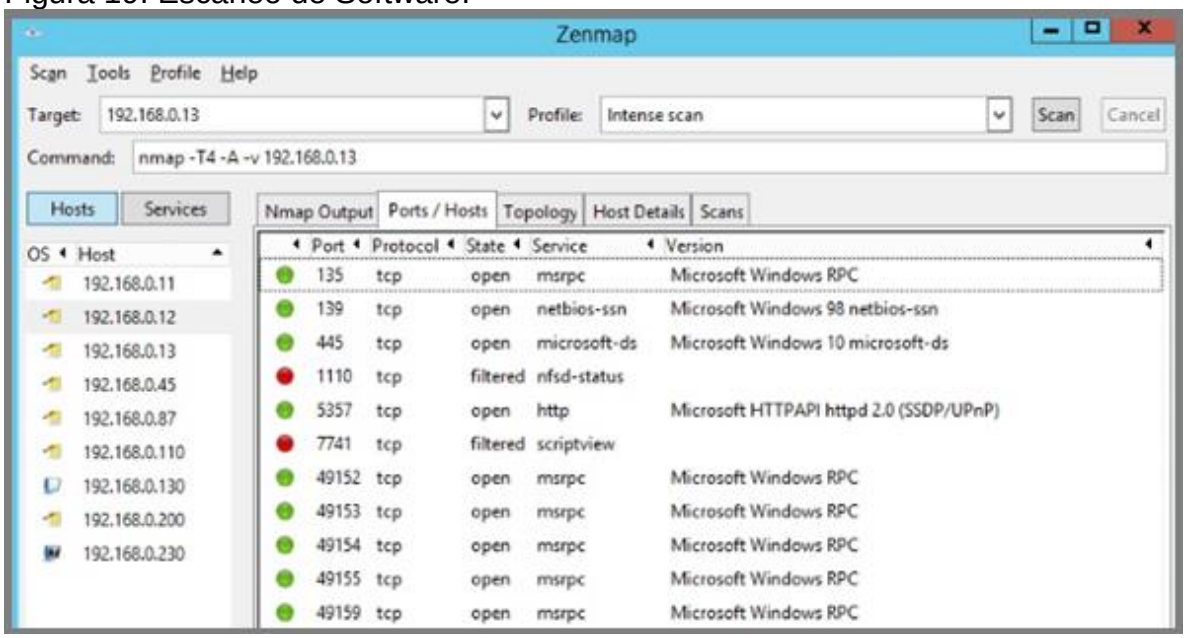
Raw packets sent: 1817 (80.646KB) | Rcvd: 1078 (47.600KB)

Este resultado se arrojó desde la IP del servidor:

Starting Nmap 7.00 (https://nmap.org) at 2015-11-27 18:04 Hora est. Pacífico, Sudamérica
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:04
Completed NSE at 18:04, 0.00s elapsed
Initiating NSE at 18:04
Completed NSE at 18:04, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 18:04
Completed Parallel DNS resolution of 1 host. at 18:04, 0.06s elapsed
Skipping SYN Stealth Scan against 192.168.0.230 because Windows does not support scanning your own machine (localhost) this way.
Initiating Service scan at 18:04
Skipping OS Scan against 192.168.0.230 because it doesn't work against your own machine (localhost)
NSE: Script scanning 192.168.0.230.
Initiating NSE at 18:04
Completed NSE at 18:04, 0.00s elapsed
Initiating NSE at 18:04
Completed NSE at 18:04, 0.00s elapsed
Nmap scan report for 192.168.0.230
Host is up.
PORT STATE SERVICE VERSION
1/tcp unknown tcpmux
3/tcp unknown compressnet
4/tcp unknown unknown
6/tcp unknown unknown
7/tcp unknown echo
9/tcp unknown discard
13/tcp unknown daytime
17/tcp unknown qotd
19/tcp unknown chargen
20/tcp unknown ftp-data
21/tcp unknown ftp
22/tcp unknown ssh
23/tcp unknown telnet
24/tcp unknown priv-mail
25/tcp unknown smtp

En la opción *Hosts* Describe los programas que se están utilizando, los puertos y cuáles en cada ordenador, en este caso la mayoría están abiertos

Figura 19. Escaneo de Software.



Fuente del autor.

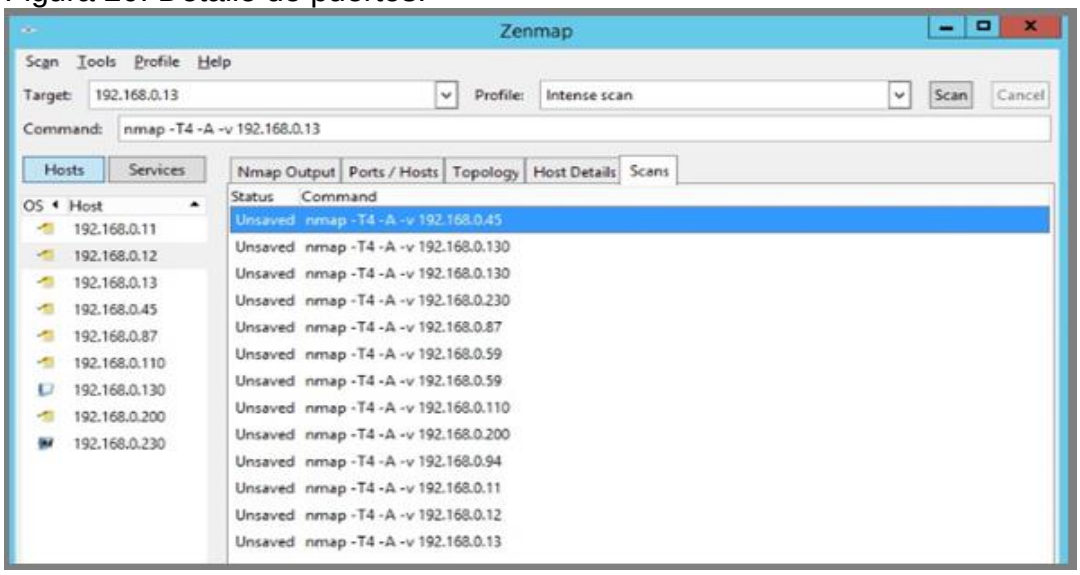
Se evidencia en Figura 23. Escaneo de Software que los puertos abiertos están señalados de color verde, lo cual genera gran vulnerabilidad para los equipos ya que están expuestos a un sinnúmero de amenazas para el sistema.

Puerto 135 lo comparten DCOM, programador de tareas y MSDTC, al parecer se tiene alguno de estos servicios el puerto permanece abierto y aceptando conexiones entrantes.

Puertos 139 y 445, los equipos tienen *NetBios* habilitado, si *NetBios* está deshabilitado, sólo se escuchará mediante el puerto 445.

Se evidencia los detalles de los puertos encontrados en la red

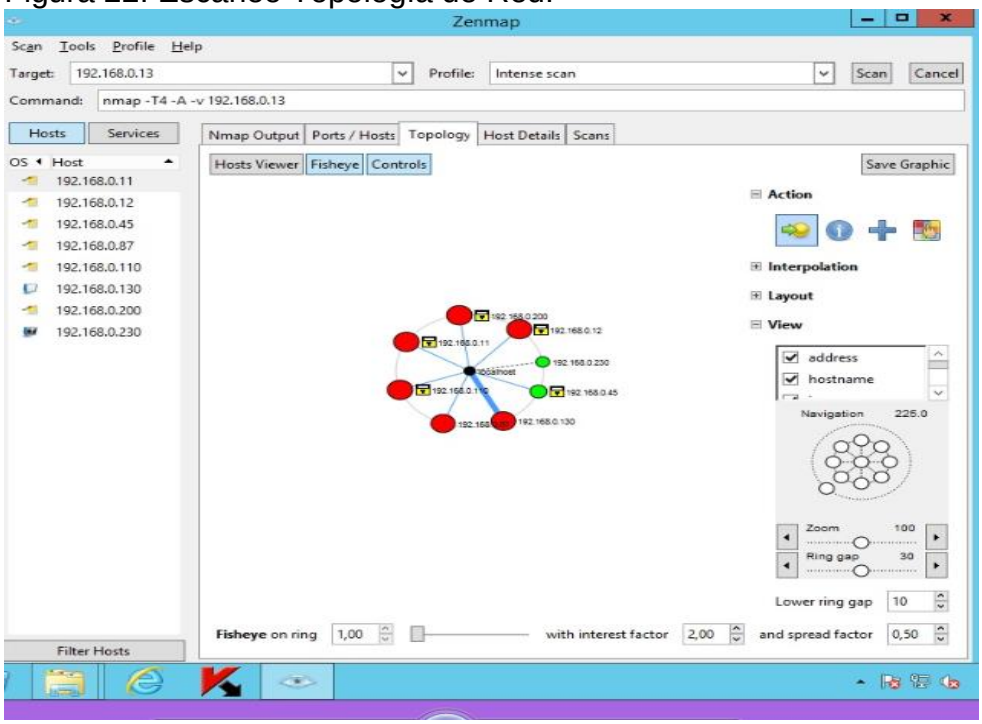
Figura 20. Detalle de puertos.



Fuente del autor.

Se puede observar la topología de la red:

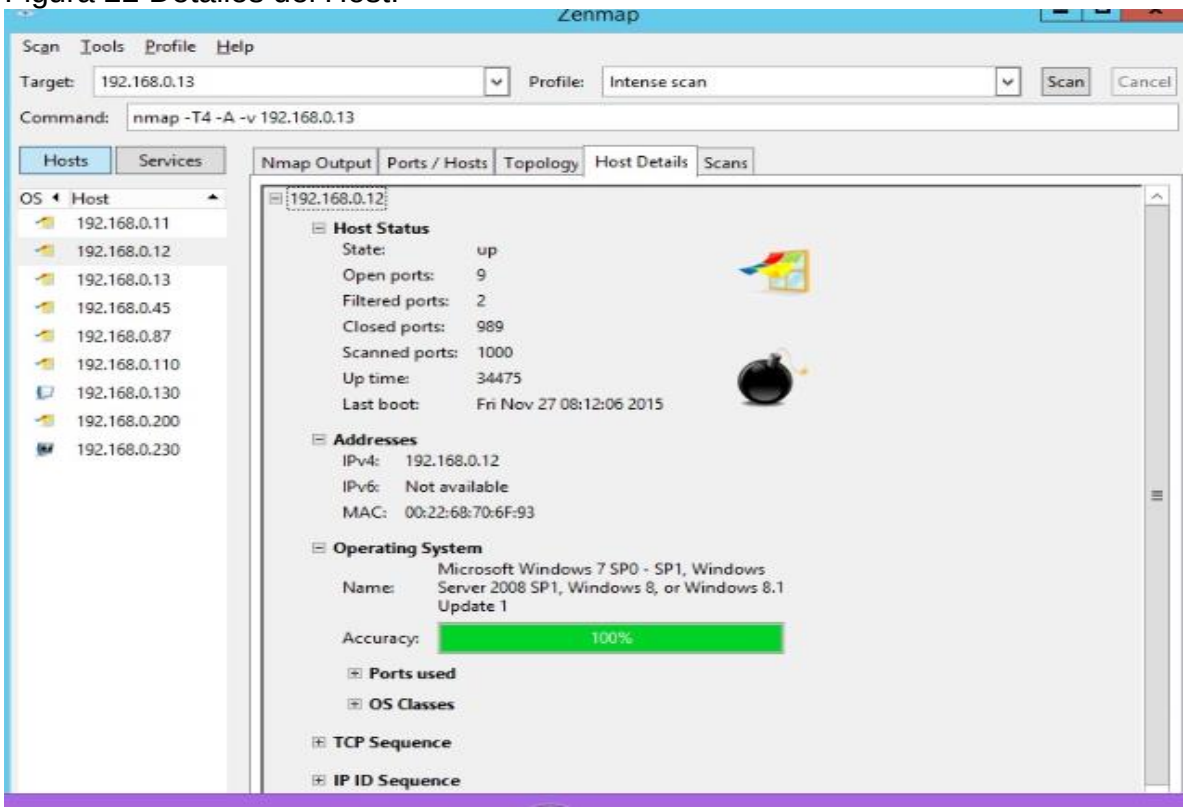
Figura 22. Escaneo Topología de Red.



Fuente del autor

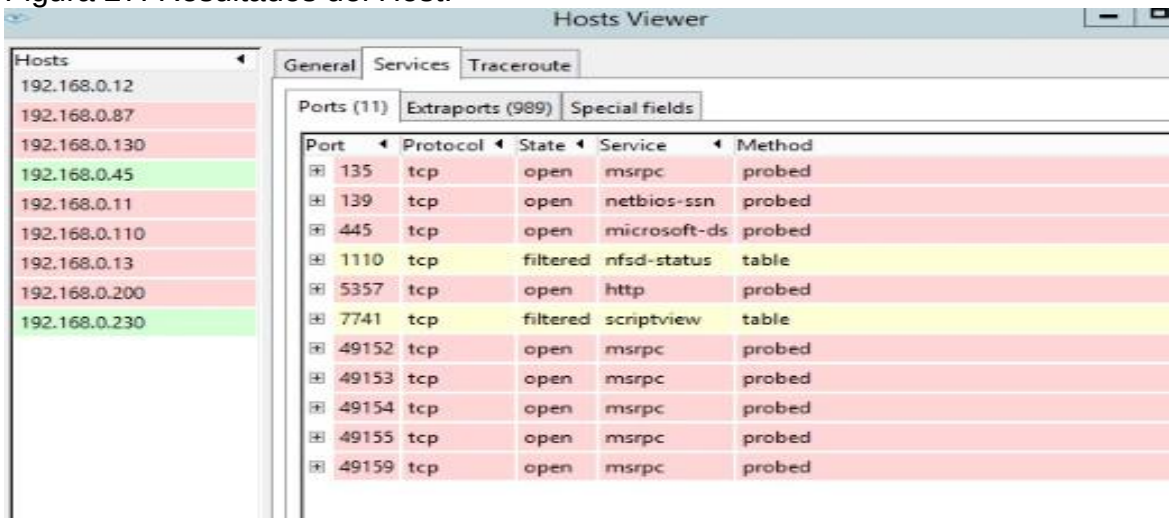
Se puede observar los detalles del host.

Figura 22 Detalles del Host.



Fuente del autor.

Figura 27. Resultados del Host.



Fuente del autor.

En General se detectaron vulnerabilidades de la red como: evidencia de los nombres de los equipos, el sistema operativo que se está usando y los puertos de los equipos, al aplicar algunos scrips se podría a acceder a información de los equipos como contraseñas.

Estas son algunas de las vulnerabilidades encontradas, ausencia de Contraseñas o de fácil detección, falta de Registros de eventos, hallazgo de puertos abiertos o sin control, carencia en copias de Respaldo o Backups las cuales deben realizarse de forma periódica dependiendo la organización, debe existir una política de respaldo y restauración, revisarse por lo menos una vez al mes si se está realizando el respectivo respaldo a prueba de fallos.

8 CONCLUSIONES

- . Se detectaron vulnerabilidades de la red como el nombre del equipo, el sistema operativo que se está usando y los puertos de los equipos, se encontraron falencias relacionadas con la seguridad de la información, seguridad en los sistemas operativos y en las redes

- Se evaluó, analizó y se documentó los posibles riesgos o amenazas, por medio de herramientas como la observación directa, entrevistas, encuestas y el monitoreo a los usuarios de la Secretaria de Educación y cultura de Sogamoso.

- la Secretaria de Educación y Cultura debe enfocar parte de su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuenta para hacerle frente a posibles ataques informáticos y luego no se pueda traducir en pérdidas de información

- La seguridad informática es de vital importancia en la Secretaria de Educación y Cultura de Sogamoso, por lo cual es indispensable implementar estrategias metodológicas de Seguridad orientadas a brindar protección contra las contingencias y riesgos.

- Se evidenció, el compromiso del personal de la secretaria en relación a la seguridad informática, se realizó el cambio de claves las cuales se crearon más robustas y de difícil detección.

9 RECOMENDACIONES

Implementar un plan de gobierno de las tecnologías de Información, enfatizando sobre las vulnerabilidades a las que están expuestos, los diferentes riesgos potenciales y la importancia de este proceso para la Secretaria de Educación y Cultura de Sogamoso.

Realizar periódicamente un *pentesting* para detectar las diferentes vulnerabilidades a que puede estar expuesta la Secretaria, de tal forma que podamos ver los puntos más débiles con el pensamiento de un atacante.

Actualizar periódicamente los sistemas con las últimas versiones de parches de seguridad, actualización de antivirus y actualizar al personal frente a los últimos ataques que se estén presentando, de esta manera estar alerta y así poder evitarlo

Los informes del *Pentesting* deben ser analizados por el responsable de los sistemas de información para tomar las medidas correctoras adecuadas.

Se debe documentar en orden estructurado un registro de eventos de uso de los sistemas de información, para obtener un control que permita optimizar la seguridad de la información.

BIBLIOGRAFÍA

Archivo General de la Nación Colombia Ley 1273 de 2009. [Internet]: [Consultado 2016 noviembre 05] Disponible en <http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_1273_DE_2009.pdf>

Curso gratuito *Pentesting, DragonJar* [Internet]: [Consultado 2017 enero 22] Disponible en <https://www.dragonjar.org/como-realizar-un-pentest.xhtml>

Curso gratuito *Pentesting, DragonJar* [Internet]: [Consultado 2017 febrero 15] Disponible en <https://www.dragonjar.education/leccion/introduccion-al-pentesting-documentacion/>

Delta Asesores, Delitos informáticos en Colombia [Internet]: [Consultado 2016 noviembre 05] Disponible en <http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia>

Facultad de Ingeniería, UNAM Universidad Nacional Autónoma de México, Laboratorio de redes y seguridad, Estándares y Normas de seguridad. [Internet]: [Consultado 2016 abril 2] Disponible en <http://ccia.ei.uvigo.es/docencia/SSI/normas>

Facultad de Ingeniería, UNAM Universidad Nacional Autónoma de México Seguridad Informática [Internet]: [Consultado 2016 noviembre 22] Disponible en <http://revista.seguridad.unam.mx/numero-18/pruebas-de-penetraci%C3%B3n-para-principiantes-5-herramientas-para-empezar>

Guía avanzada de Nmap [Internet]: [Consultado 2017 noviembre 20] Disponible en <http://www.csirtcv.gva.es/sites/all/files/downloads/Guia_Avanzada_Nmap.pdf>

Guía de Seguridad en las Tics, guía avanzada de Nmap [Internet]: [Consultado 2017 noviembre 20] Disponible en <https://www.kalerolinex.com/wp-content/uploads/2015/01/Guia_Avanzada_Nmap.pdf?cv=1 página 9>

Hack players, publicación de la versión 7 de Nmap, escáner de Redes [Internet]: [Consultado 2017 diciembre 03] Disponible en <http://www.hackplayers.com/2015/11/llega-la-version-7-de-nmap.html>

Instituto Colombiano de Normas Técnicas. Normas colombianas para la presentación de trabajos de investigación [Internet]: [Consultado 2017 marzo 12] Disponible en <http://66.165.175.235/campus18_20151/*file.php*/85/entorno_de_conocimiento/NTC14862008.pdf>

Nmap security scanner, Detección de Sistemas operativos Redes [Internet]: [Consultado 2017 diciembre 03] Disponible en <https://nmap.org/man/es/man-os-detection.html>

PUERTA CANO Juan E. BUILES Yuliet. GARCIA Fabio. Analistas Desarrolladores de Jeduca S.A.S, Pruebas de penetración con Nmap Redes [Internet]: [Consultado 2017 diciembre 03] Disponible en <https://es.slideshare.net/juanestebanpuertacano/pruebas-de-penetracin-nmap>

RAMIREZ VILLEGAS Gabriel Mauricio y CONSTAIN MORENO Gustavo Eduardo Director nacional UNAD, Diseñador de material didáctico Modelos y estándares de seguridad informática [Consultado 2017 marzo 12] Disponible en <http://datateca.unad.edu.co/contenidos/233002/Periodo_2014-2/Entorno_de_conocimiento/material didactico.pdf>

Secretaria de Educación y Cultura de Sogamoso, Información acerca de la Entidad [Internet]: [Consultado 2016 Octubre 10] Disponible en <http://sem-sogamoso-boyaca.gov.co>

Ubuntu manuales, Nmap - Herramienta de exploración de redes y de sondeo de seguridad, puertos [Internet]: [Consultado 2017 diciembre 03] Disponible en <http://*manpages.ubuntu.com/manpages/trusty/es/man*1/nmap.1.html>

ANEXOS

Anexo A. Formato de Encuesta.

ENCUESTA DE SEGURIDAD INFORMATICA APLICADA A LOS FUNCIONARIOS DE LA SECRETARIA DE EDUCACION Y CULTURA DE SOGAMOSO

1 Usted tiene conocimiento acerca de que es la seguridad Informática?
Si_____ No _____ No se_____

2 Conoce algún plan de seguridad informática implementado en la secretaria de Educación y cultura de Sogamoso.
Si_____ No _____ No se_____

3 Usted ha permitido el acceso a la información que maneja sólo a personas debidamente autorizadas?
Si_____ No _____ No se_____

4 ¿la información que usted maneja tiene los privilegios de confidencialidad, integridad y disponibilidad?
Si_____ No _____ No se_____

5. Usted como usuario a accedido a todos los datos permitidos?
Si_____ No _____ No se_____

6 Se tiene definida una política para las copias de seguridad de la información?
Si_____ No _____ No se_____

7 Se tiene definida una política de restauración de los sistemas en caso de ataques informáticos?
Si_____ No _____ No se_____

8 Tiene conocimiento acerca de algún tipo de seguridad en la red?
Si_____ No _____ No se_____

9 La Secretaría cuenta con antivirus actualizado?
Si_____ No _____ No se_____

10 La secretaria cuenta un control de las claves de los computadores?
Si_____ No _____ No se_____

Gracias.

Anexo B. Evidencia: socialización de seguridad informática aplicada a los funcionarios de la secretaria de educación y cultura de Sogamoso.

Anexo C. Carta aceptación de prueba de Pentesting

Sogamoso, 12 octubre 2015

Señora:
NUBIA CARMENZA MONROY BARRETO
Secretaria de Educación y Cultura
SOGAMOSO.

Cordial saludo,

Amablemente solicito el permiso para realizar una práctica en el área de redes, con el fin de determinar las vulnerabilidades presentes en la red de sistemas de la secretaria de Educación y cultura por medio de un Pentesting y así poder evaluar los resultados obtenidos y proponer soluciones para los riesgos encontrados. Estudio realizado como proyecto de grado para obtener el título de Especialista en Seguridad Informática.

Agradezco su colaboración,

Atentamente,

Wilson Escobar Lemus
C.c. 9396906
ESTUDIANTE ESPECIALIZACION SEGURIDAD INFORMATICA
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

Nubia Monroy
aprobado
16-3-15